Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Dirección General de Estudios de Posgrado
Facultad de Ingeniería Electrónica y Eléctrica
Unidad de Posgrado

Desarrollo e implementación de un sistema de control de acceso a redes inalámbricas mediante RADIUS

TESIS

Para optar el Grado Académico de Magíster en Telecomunicaciones con mención en Sistemas de Información en Telecomunicaciones

AUTOR

Elvis Daniel ESPINOZA ARANA

ASESOR

Víctor Manuel CRUZ ORNETTA

Lima, Perú

2018

Referencia bibliográfica

Espinoza, E. (2018). *Desarrollo e implementación de un sistema de control de acceso a redes inalámbricas mediante RADIUS*. [Tesis de maestría, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Unidad de Posgrado]. Repositorio institucional Cybertesis UNMSM.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA

UNIDAD DE POSGRADO

Calle Germán Amezaga N.° 375 Lima (Perú)
Telefóno (51 – 1) 6197000 Anexo 4204
Correo: postfiee@gmail.com

«AÑO DEL DÍALOGO Y RECONCILIACIÓN NACIONAL»

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAGÍSTER EN TELECOMUNICACIONES CON MENCIÓN EN SISTEMAS DE INFORMACIÓN EN TELECOMUNICACIONES

Siendo las 18:00 horas. del 11 de julio de 2018, en el salón de Grado de la Facultad de Ingeniería Electrónica y Eléctrica, el Jurado de Examinador presidido por el Dr. Santiago Rojas Tuya, Mg. Wilbert Chávez Irazabal, Mg. Carlos Alberto Sotelo López, Mg. Daniel Díaz Ataucuri y el Dr. Víctor Manuel Cruz Ornetta.

Se reunió para la sustentación oral y pública de la Tesis para optar el Grado de Académico de Magíster en Telecomunicaciones con Mención en Sistemas de Información en Telecomunicaciones, que solicitó el alumno **Elvis Daniel Espinoza Arana**, el cual procedió hacer la exposición oral y pública de su Tesis Titulada **"DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO A REDES INALÁMBRICAS MEDIANTE RADIUS."**

Concluida la exposición, se procedió a la evaluación correspondiente, habiendo obteniendo la siguiente calificación:

DE " CATORCE (14) "
LETRAS NÚMERO

A continuación, el Presidente Jurado recomienda que la Unidad de Posgrado proceda con el trámite correspondiente para que se otorgue el Grado Académico de Magíster en Telecomunicaciones con Mención en Sistemas de Información en Telecomunicaciones al alumno **Elvis Daniel Espinoza Arana**.

Siendo las 20:00 h. se levantó la Sesión, recibiendo el graduado las felicitaciones de los señores miembros del Jurado y público asistente.

Dr. SANTIAGO ROJAS TUYA
Presidente

Mg. WILBERT CHÁVEZ IRAZABAL
Miembro

Mg. CARLOS ALBERTO SOTELO LÓPEZ
Miembro

Mg. DANIEL DÍAZ ATAUCURI
Miembro

Dr. VÍCTOR MANUEL CRUZ ORNETTA
Miembro Asesor

Dedicatoria

A Dios porque cada me dio la certeza de vivir con propósito,

A mi Padre Julián quien le agradezco cada minuto de su tiempo y sabiduría

A mi Madre Elvira quien con su amor me enseña a tener Fe en la vida

A mis hermanos Yuliana y Billy quienes siempre estarán conmigo

AGRADECIMIENTO

Al Dr. VÍCTOR MANUEL CRUZ ORNETTA Decano de la Facultad de Ingeniería Eléctrica y Electrónica por su apoyo en el desarrollo de este trabajo y asesoramiento de esta Tesis

ÍNDICE GENERAL

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

El objetivo del presente trabajo fue investigar el desarrollo de un diseño para la implementación de sistema de seguridad Inalámbrica que permitiera controlar la actividad de los usuarios al realizar un tráfico de datos en el Instituto Geofísico del Perú, para ello se realizó un estudio del protocolo RADIUS. Este protocolo trabaja con estándares de seguridad como el AAA, y con estas características particulares fue posible la adaptación y uso de la aplicación eduroam.

Durante el proceso de ejecución del proyecto piloto del nuevo sistema de control inalámbrico se logró implementar en la sede principal de monitorio sísmico, este proyecto partió de la Oficina de Tecnologías de Información de Datos Geofísicos – OTIDG. servicio con la aplicación eduroam alrededor de 40 investigadores pudieron ser los primeros usuarios en experimentar la bondades dentro y fuera de la Institución con otras entidades que utilizan este servicio, siendo en su mayoría Centros de Investigación y en otros casos Aeropuertos Internacionales.

El proyecto inicial mostro las fortalezas logradas con una gran percepción de los usuarios que usaron el servicio lo cual se reflejó en la encuesta virtual que recopilo la percepción y sensación de confort al realizar uso de este servicio. Cabe resaltar que en su gran mayoría los encuestados no solo tuvieron buenas experiencias al hacer uso de eduroam puesto que facilito el acceso y elimino el tema burocrático de accesibilidad en otras entidades, sin no que también la percepción de confianza que tuvo el usuario fue aceptable logrando tener una apoyo de esta implementación por parte de la Alta Dirección del IGP.

Los resultados de las encuestas fueron sometidos usando un paquete estadístico SPSS 20 y mediante de pruebas de CHI-CUADRARO se corrobora la aceptación de las variables en los resultados mostrados estadísticamente.

En conclusión el estudio demostró que la Un Sistema de Seguridad de Control de Acceso con RADIUS produce efectos que determina el grado de autenticación y autorización en el control de tráfico inalámbrico.

Palabras claves:

- RADIUS
- EDUROAM
- PROTOCOLO EAP
- LDAP
- NAS

ABSTRACT

The objective of the present work was to investigate the development of a design for the implementation of wireless security system that allowed to control the activity of the users when carrying out a data traffic in the Geophysical Institute of Peru. A study of the RADIUS protocol . This protocol works with security standards such as AAA, and with these particular characteristics it was possible to adapt and use the eduroam application.

During the execution of the pilot project of the new wireless control system, the project was implemented at the main site of monitoring of seismic, this project started from the Office of Geophysical Data Information Technologies (OTIDG). Service with the application eduroam about 40 researchers could be the first users to experience the benefits inside and outside the Institution with other entities that use this service, being mostly Research Centers and in other cases International Airports.

The initial project showed the strengths achieved with a great perception of the users who used the service which was reflected in the virtual survey that collected the perception and feeling of comfort when using this service. It should be noted that in the vast majority of respondents not only had good experiences when using eduroam since it facilitated access and eliminated the bureaucratic issue of accessibility in other entities, but also that the user's perception of trust was acceptable To have support from this implementation by the Senior Management of the PGI.

The results of the surveys were submitted using a statistical package SPSS 20 and by means of tests of CHI-QUADRARO the acceptance of the variables in the results shown statistically is corroborated.

In conclusion, the study showed that an Access Control Security System with RADIUS produces effects that determines the degree of authentication and authorization in wireless traffic control.

Keywords:

- RADIUS
- EDUROAM
- PROTOCOLO EAP
- LDAP
- NAS

CAPITULO 1: INTRODUCCION

1.1 Situación Problemática

Durante la última década del Siglo XXI hemos experimentado una importante transformación en el despliegue de la tecnología WIFI, el cual inicialmente era una extensión de la red cableada tradicional, sin embargo con el auge de los nuevos dispositivos tales como tabletas, teléfonos inteligentes, impresoras inalámbricas, consolas de juego y computadoras personales portátiles sin puerto de red LAN integrado, viene siendo el medio preferido y que en estos días se le preste una particular atención a la forma de su despliegue.

La masificación de los dispositivos móviles ha dado como resultado el bajo costo de hardware, siendo así un estándar en todo dispositivo móvil inteligente que necesariamente debe poder contar con tecnología WIFI.

Esta alta demanda de estos dispositivos móviles que usan tecnología WIFI plantea nuevos desafíos no resueltos aun en los ámbitos corporativos como en los espacios públicos haciendo participe a los administradores de red en optar por una solución integral y que brinde la seguridad y confidencialidad de toda transferencia de datos a través de un acceso inalámbrico. (Vázques, 2014, p.27)

El crecimiento de la tecnología inalámbrica innovó y mejoro el acceso a la red, sin embargo se evidencio mayores amenazas y vulnerabilidad de la red de datos que ponían en riesgo los activos de información en una corporación y la suplantación de identidad así como el robo informáticos. (El Yaagoubi, 2012).

Implementar controles administrativos, técnicos y físicos necesarios para proteger la confidencialidad, integridad y disponibilidad de los activos de información, los controles se manifiestan a través de políticas, procedimientos, estándares, instructivos y guías, entre otros.

Gestionar los riesgos, considerando técnicas y herramientas para realizar el inventario de activos, análisis de riesgos, clasificación de la información y concientización en seguridad. Los activos de información son clasificados y luego analizados sus riegos mediante identificación de amenazas y vulnerabilidades relacionadas a las categorías de activos, así como las salvaguardas adecuadas para mitigar los riesgos de forma priorizada

Por tal motivo las herramientas de seguridad informática en el campo de las telecomunicaciones juegan un papel protagónico en la infraestructura con igual o mayor importancia del que representa la seguridad física misma, ya que se debe de proteger servicios importantes como lo son flujo, almacenamiento y manejo de información entre otros. (Ventura, 2008)

Generalmente, al realizar la implementación de puntos de acceso inalámbrico en la red de una organización de tipo corporativo, se opta por un protocolo y un método de acceso que cumpla con las políticas definidas por dicha organización. Se definen también, en esta elección, las características que deben cumplir los dispositivos de los usuarios, excluyendo a todos los equipos que no cumplen con dichas características.

Así, podríamos decir que hoy en día, cualquier organización (académica o comercial) con intención de organizar y mejora su sistema de Seguridad de Control de Acceso inalámbrico con RADIUS debe configurarse bajo una plataforma en Linux para determinar el grado de confiabilidad seguridad y autenticidad en el control de tráfico inalámbrico de información

1.2 Formulación del Problema

1.2.1 Problema General

¿Qué efectos produce un sistema de Seguridad de Control de Acceso con RADIUS en el grado de autenticación y autorización en el control de tráfico inalámbrico?

1.2.2 Problemas específicos

1.2.2.1 Problema específico 1: ¿Qué resultados produce un sistema de Seguridad de Control de Acceso con RADIUS en el grado de autenticación del control de tráfico inalámbrico de información?

1.2.2.2. Problema específico 2: ¿Cómo repercute un sistema de Seguridad de Control de Acceso con RADIUS en el grado de autorización del control de tráfico inalámbrico de información?

1.2.2.3. Problema específico 3: ¿Cómo repercute el Desarrollo de un Modelo de Administración y gestión de usuarios en el control de tráfico inalámbrico?

1.3 Justificación Teórica

En esta investigación nos permitirá conocer las vulnerabilidades que afectan a la red e incrementar los niveles de seguridad para acceder a la red inalámbrica del IGP, con la implementación de un servidor RADIUS, el cual autenticara al usuario al momento de su acceso.

1.4 Justificación Práctica

Desde el punto de vista práctico esta investigación ha demostrado que la implementación de un sistema RADIUS genera las siguientes bondades:

- Otorgar mayor seguridad en la red para el usuario y autenticación a cada uno de estos y brindar seguridad reduciendo la filtración de usuarios no autorizados a la Institución.

- Escalabilidad de esta nueva implementación con un servidor RADIUS a la red inalámbrica ya existente con la aplicación eduroam y mostrarnos en el mundo como una Institución de Confianza para los investigadores internacionales.

1.5 Objetivos de la Investigación

1.5.1 Objetivo General

Desarrollar e Implementar los efectos que produce un sistema de Seguridad de Control de Acceso con RADIUS en el grado de autenticación y autorización del control de tráfico inalámbrico de información.

1.5.2 Objetivos Específicos

1.5.2.1 Objetivos Específicos 1. Analizar los efectos que produce un sistema de Seguridad de Control de Acceso con RADIUS en el grado de autenticación en el control de tráfico inalámbrico.

1.5.2.2 Objetivos Específicos 2. Analizar los efectos que produce un sistema de Seguridad de Control de Acceso con RADIUS en el grado de autorización en el control de tráfico inalámbrico.

1.5.2.3 Objetivos Específicos 3. Desarrollar un modelo de sistema administrativo y gestión de usuarios en el control de tráfico inalámbrico.

CAPITULO 2: MARCO TEÓRICO

2.1 Marco Filosófico o epistemológico de la Investigación

Seguridad es una necesidad básica. Estando interesada con la preservación de la vida y las posesiones, es tan antigua como la vida. Los conceptos de seguridad es encuentran ya en el inicio de la escritura. La evidencia escrita más temprana de conceptos relacionados con la seguridad se encuentra en códigos legales, tales como el Sumerio (3.000ac) o el de Hammurabi (2.000ac). Más tarde, aparece en obras generalmente refiriéndose al arte de la guerra y gobierno. La Biblia, Homero, Sun Tzu, Cicerón, Virgilio, Cesar, Frontino, Suetonio, Joseph, Vegetio, son ejemplos relevantes de obras de autores donde ciertas evidencias de temas y principios de seguridad son halladas. (Manunta, 2006)

Otra evidencia puede ser encontrada en la arqueología y la antropología. Por ejemplo, podemos razonablemente asumir que la cultura y habilidades de seguridad son reconocibles en actuales culturas primitivas que son muy cercanas a las de nuestros ancestros. Como informan los antropólogos, las organizaciones sociales primitivas revelan un profundo conocimiento y sofisticada aplicación de los principios y funciones básicas de seguridad. Desde su nacimiento, las personas son instruidas, vía tradición y entrenamiento, y/o vía imitación, en las habilidades para la seguridad. Los bebes son instruidos en no llorar en las proximidades de un enemigo, y son entrenados desde su infancia en reconocer y evitar peligros, a dar alarma, y a esconderse y refugiarse en caso de necesidad. Los hombres jóvenes físicamente fuertes (y a veces las mujeres) son requeridos para mantener erectas, guardar, mantener y defender barreras físicas. Los asentamientos

son reforzados con fuegos y primitivas empalizadas (hechas de ramas de plantas espinosas), que son frecuentemente adornadas con las cabezas de enemigos muertos, signos mágicos y tabús, con el fin de incrementar el valor "intimidatorio". Pueblos primitivos domesticaron animales para obtener alarma y soporte, para reaccionar organizadamente como equipos, de acuerdo con bien planeadas y ensayadas tácticas, cuando el combate era considerado inevitable, o cuando la potencial pérdida fuera letal. (Leonardo, 2014, p.3)

La evidencia de medidas de seguridad acompaña cada descubrimiento arqueológico. Cerraduras, puertas fuertes, ventanas selladas, trampas, cajas fuertes, sistemas de alarma, barreras físicas y escudos son conocidos y usados desde el principio de la civilización. La más antigua cerradura conocida data de 4.000ac, y fue encontrada en el palacio de Sargon, Khorsabad, cerca de Nineveh. En el mismo periodo, el dibujo de una cerradura fue realizado en el templo de Karnak, en el valle del Nilo. En el 1.000ac, el dios egipcio Anubi fue representado con una llave en su mano derecha. La caja fuerte más antigua conocida fue encontrada en Pompeya y datada en el IIac; realizada de madera con bandas de hierro, tiene una mecánica muy sofisticada. Es muy similar, en su concepción, a las cajas utilizadas hasta el siglo pasado. (Manunta, 2006)

De acuerdo con la evidencia anterior, no existe duda de que los conceptos de alertar, evitar, detectar, alarmar y reaccionar son tan viejos como la vida misma, siendo una parte esencial de la pugna diaria por la vida, y están fundados en el instinto básico de supervivencia. Primitivos seres humanos estaban ciertamente alerta sobre los peligros, y antes de que métodos defensivos emergieran, sólo podían reaccionar como los animales, intentando tanto evitar las amenazas más temidas, o eliminado su causa, dentro del bien conocido patrón de "luchar o huir (flight or fight)". (Manunta, 2006)

Probablemente, el próximo paso en la evolución de la seguridad fue la emergencia de la especialización, primero por la división entre la seguridad interna y externa, y después entre la seguridad privada y pública. Con la aparición del estado y la confianza de su defensa a un organizado ejército, la responsabilidad de la seguridad interna se relevó gradualmente de la fuerza militar a la fuerza civil.

Conceptos relacionados a la seguridad, están relacionados en nuestros días a la protección de los activos de información por lo que se ha de profundizar sobre el concepto de la seguridad perimetral como primera barrera en nuestra red de información.

Seguridad Perimetral

Seguridad perimetral es una estrategia para proteger los recursos de una organización conectada a la red, sin ser un componente aislado, así también la realización de práctica de las políticas de seguridad, por lo que sin una política de seguridad, esto no tendría ninguna validez, la implementación de una seguridad perimetral condiciona y da credibilidad a una organización en Internet, por ello se hace mención que está compuesta por software, hardware y políticas para proteger la red en la que se tiene confianza (Intranet) de otras redes de las que no se tiene confianza (extranet, internet). Definiremos conceptos tales como perímetro el cual es la frontera fortificada de una red, incluye routers, Firewalls o cortafuegos, sistemas de detección de intrusos, VPN´s, DMZ o zonas desmilitarizadas.

El Firewall, analiza la composición del paquete tanto de entrada como de salida de la Red debido que al realizar el análisis se obtendrá información de la capa de red y transporte, finalizado el análisis tomara las acciones correspondientes. (Sistemas de Seguridad por Contenidos – TECSUP 2013)

Listas de Acceso

Dentro de los conceptos de seguridad incluimos el uso de las listas de acceso, esta herramienta es de gran efectividad para el control de la red. Estas listas añaden flexibilidad para filtrar el flujo de paquetes hacia dentro o hacia fuera de las interfaces de un router. Tal control puede ayudar a limitar el trafico de red y restringir el uso de la red para ciertos usuarios o dispositivos. Las listas de acceso o Access List diferencian al trafico de paquetes en categorías que permiten o deniegan otras características, estas se pueden utilizar para identificar paquetes por prioridad o cola personalizada y también restringir o reducir el contenido de las actualizaciones de ruteo.

Las listas de acceso ACL , son una técnica de filtrado de paquetes, que consiste en una lista de ordenes ejecutadas secuencialmente a la llegada/salida de cada paquete en las interfaces del router con las opciones permit o deny al cumplir la condición especificada en la secuencia según la información de la cabecera del paquete IP y de transporte. Al realizar en el propio router, suelen ser rápidas frente a otra técnica de filtrado (Seguridad Perimetral I – TECSUP 2013)

IDS e IPS

Las técnicas de ataques continuamente están avanzando y vulnerando las redes que no cuenten con un debido nivel seguridad. Actualmente los ataques están dirigidos a vulnerar la capa de aplicación que según reportes de vulnerabilidad emitidos por la CERT están siendo cada vez mas frecuentes. Para contrarrestar estos peligros es necesario implementar soluciones de detección y prevención de intrusos IDS e IPS

Al mencionar vulnerabilidad se hace mención a la violación de una política de seguridad. Esto puede deberse a reglas de seguridad inadecuadas o a problemas dentro del mismo software. En teoría, todos los sistemas de ordenadores tienen vulnerabilidades, de cuya seriedad depende que sean o no usadas para causar un daño al sistema.

Estas vulnerabilidades poseen diversos grados de daños. Por eso es importante estar preparados para la prevención, detección y reparación, por ello pensamientos erróneos como: “Mi sistema no es importante para un cracker”, “Estoy protegido pues no abro archivos con virus que no conozco”, “Como tengo antivirus estoy protegido” ó “Como dispongo de un Firewall no me contagio”, son muchas de la ideas por las que se parte para evitar una análisis exhaustivo e invertir en seguridad.

Todo esto ha llevado a desarrollar herramientas de monitoreo asi como los IDS, los cuales se encargan de detectar anomalías en el trafico. Estas anomalías son indicios de ataques o intentos, usando sensores coleccionan el tráfico.

Los IDS actúan como supervisores de la actividad del tráfico. Su estructura de funcionamiento poseen las capacidades de analizar el tráfico y sacar conclusiones.

En un mundo real, un auditor para detectar fallas en algún proceso recurre a la documentación de los eventos de ingreso y salida. Estos documentos son formularios que son rellenados por los operadores o información registrada en las máquinas de la actividad del proceso. Al cruzar toda esta información obtendrá la causa de la falla.

Los IDS trabajan similarmente han sido diseñados con el conocimiento de la estructura del protocolo TCP/IP y de esta forma detectar si existe anomalías. Debido a que todo tráfico que circula en la red de la Empresa y de Internet es TCP/IP. Por lo tanto los IDS no reemplazan a los FIREWALL, ambos se complementan. Los Firewall fueron diseñados para revisar las conexiones de entrada y salida revisando la información de las direcciones IP, puertos. No fueron diseñados para:

- Analizar el contenido de la conexión (Virus, Vulnerabilidades)
- Detectar sospechas de intentos de ataques
- Evaluar el tráfico de congestión.

Los sistemas IDS para desarrollar sus acciones pasan por 3 etapas:

Recogida: En esta etapa es la recolección del tráfico de información, obteniéndolo de los eventos de una aplicación, de un equipo o una red. Esta información es obtenida por el Sensor del IDS.
Análisis: Luego de recoger a los datos, se procederá a su análisis, comparándolo con base de datos de anomalía o de las reglas de seguridad.
Respuesta: Según el resultado del análisis se podrá generar una alarma, reporte o una acción.
Aquí mencionamos los tipos de IDS:

- HIDS (HostIDS): IDS de Host, que monitorea la actividad de un único equipo
- NIDS (NetworkIDS): IDS basado en la red, detectando ataques en todo el segmento de la red.
- DIDS (DistributedIDS): Sistemas compuesto por una serie de NIDS, que actúan como sensores centralizando la información de posibles ataques en una unidad central que puede almacenar o recuperar los datos de una base de Datos centralizada.(Seguridad por Contenidos – TECSUP 2013)

HONEYPOTS

Ante tantas amenazas también podemos usar recursos de distracción los cuales nos ayudaran a ganar tiempo y conocer al atacante asi pues haremos mención a los HONEYPOTS
Existen diferentes conceptos de los que es un HONEYPOTS:

- Solución de atraer o engañar a los atacantes
- Tecnologías de descubrir ataques
- Computadoras para ser hackers y aprender las técnicas

Un Honeypot es un recurso de seguridad, donde el resultado dado a los atacantes es falso.

Para entender mejor el valor de los Honeypots podemos dividir en dos categorías diferentes:

- Producción: Usada para proteger su red, ellos directamente ayudan a asegurar su organización
- Investigación: Ellos son usados para coleccionar la información. Aquella información puede ser entonces usada para una variedad de objetivos, como de advertencia y predicción, o pruebas para la aplicación de la ley.

Para entender mejor, el valor de la producción de los Honeypots, usaremos el modelo de Bruce Schneier de la seguridad, que abarca tres capas: *Prevención, descubrimiento y respuesta*.

- Prevención: usado para reducir la velocidad o detener los ataques automatizados; el Honeypot LaBrea Tarpit tiene como característica hacer más lentos los ataques de TCP, como los gusanos. Contra atacantes humanos, honeypots puede utilizar armas psicológicas como engaño o fuerza de disuasión para aturdir o parar ataques.
- Descubrir: Descubrir la actividad no autorizada. Las soluciones de descubrimiento tradicionales pueden abrumar con alarmas, y aun solo algunas de las alarmas señalan ataques válidos. También muchas de las tecnologías de hoy son diseñadas para descubrir ataques desconocidos. La ayuda de Honeypots resuelve ambos de estos problemas. Los Honeypots generan muy pocas alarmas, pero cuando emiten alarmas puede estar casi seguro que algo malévolo ha pasado. El Honeypots puede descubrir también y capturar ataques desconocidos así como ataques conocidos.
- Responder: Los Honeypots puede ser usada para responder a un ataque. Si un atacante irrumpe en la organización o institución, y uno de los sistemas que ingresaron era un Honeypot, entonces la información juntada de aquel sistema puede ser usada para responder al ataque. El Honeypots puede ser usado también para ahuyentar e identificar a un atacante.

Dentro de las ventajas de usar Honeypots mencionamos las siguientes:

- Captura eficiente de información, pues coleccionan pequeñas cantidades de información.
- En vez de generar 10 000 alarmas por día, ellos pueden generar solo 10 alarmas por día, sin olvidar que solo capturan actividad maliciosa.
- Cualquier interacción con un Honeypot es la actividad más probablemente no autorizada o malévola, facilitando el análisis de los datos coleccionados y obtener la información.

Nuevas tácticas o Instrumentos que son diseñados para capturar tácticas nunca antes vistas, a su vez requieren recursos mínimos en cuanto a hardware, otro de los puntos interesantes a resaltar de estas técnicas es la codificación o IPV6, a diferencia de la mayor parte de tecnologías de seguridad (como sistemas IDS) honeypots puede trabajar en ambientes criptografiádos o IPV6.
Los Honeypots coleccionan la totalidad de la información a diferencia de otras tecnologías por lo que son simples de configurar y mantener.

Dentro de las desventajas encontradas tenemos las siguientes:

- Una vista limitada pues solo captura la actividad que directamente actúa recíprocamente con ellos. El Honeypot no captura ataques contra otros sistemas, a menos que el atacante o la amenaza actúen recíprocamente con el Honeypot.
- El riesgo de ser apoderados por el atacante y usado para dañar a otros sistemas. (Seguridad por Contenidos – TECSUP)

Virus y Antivirus

El que se considere el primer virus propiamente dicho y que fue capaz de “infectar” maquinas IBM 360 a través de una red ARPANET (el precedente de la Internet actual), fue el llamado Creeper, creado en 1972 por Robert Thomas Morris. Este parasito emitia un mensaje en la pantalla

periódicamente: “I´m a creeper… catch me if you can!” (Soy una enredadera, atrápame si puedes)
Para eliminar a Creeper se creo otro virus llamado Reaper (segadora) programado para buscarlo y eliminarlo. Este es el origen de los actuales antivirus.

Troyanos

En enero de 1975, John Walker (fundador de Autodesk) descubre una nueva forma de distribuir un juego en su UNIVAC 1108 e inadvertidamente da origen al primer troyano de la historia. El mismo recibe el nombre “Animal/Pervade”, animal ya que consistía en que el software debía adivinar el nombre de un animal en base a preguntas realizadas al usuario y; Pervade que era la rutina capaz de actualizar las copias de Animal en los directorios de los usuarios, cada vez que el mismo era ejecutado, de allí que sea un troyano.

Gusano

A finales de los setenta, John Shoch y John Hupp, investigadores del centro de investigación Xerox de Palo Alto, California intentaron darle un uso practico a los CoreWars, creando un programa que se encargaba de las tareas de mantenimiento y gestión nocturnas, propagándose por todos los sistemas del centro. Lamentablemente este “trabajador virtual” bautizado como worm (haciendo mención a la novela The Shockwave Rider, escrita en 1975 por John Brunner) se extendió por toda la red y causo grandes problemas, por lo que se decidió la eliminación completa del mismo.

Mientras que los sistemas libres de UNIX (Linux y los sistemas BSD), han sido los blancos de varios gusanos estos últimos años. Aunque estos gusanos no han afectado el funcionamiento y la seguridad de Internet comparado a los incidentes del gusano de Windows.

Los sistemas libres de Linux como blanco para los gusanos es probablemente debido a tres factores:

- Son una opción como plataforma de trabajo para muchos atacantes
- Unix trabaja con scripting y forman redes, que son activos para los sistemas del gusano.
- Compiladores que están libremente disponibles para los sistemas, significando que los atacantes pueden desarrollar los componentes binarios del gusano para el uso en estos sistemas.

ADMworm-v1 1998

En mayo de 1998, el grupo subterráneo “ADM” de la seguridad escribió y lanzo los archivos ADMworm-v1. Este gusano ataco los sistemas de Linux y utilizo el BIND 8.1 que tenía la vulnerabilidad 4.9.8 desbordando y obteniendo acceso de administrador el gusano creaba una cuenta privilegiada, para que el atacante podría volver luego para ingresar.
El gusano fue compuesto de varios componentes. Algunos de los componentes, fueron escritos como los Shell scripts y se ocultaba en execuables compilados. La herramienta del exploit, contenia un generado IP (Sistemas de Cifrado y Autenticación – TECSUP 2013)

Los sistemas de seguridad son cada vez más automáticos, particularmente aquellos de detección y comunicación de siniestros, y en una extensión menor, aquellos relacionados con la valoración, la decisión y la reacción. Los avances en la miniaturización se reflejan en los equipos de seguridad que cada vez son más pequeños, más baratos, más fácilmente instalados y mantenidos, y más confiables. Pero todavía, debería ser reconocido que la tecnología, aunque importante y sinérgica con la aplicación de los principios de la seguridad, no ha añadido ningún nuevo concepto a aquellos ya conocidos anteriormente. Por el contrario, parece que ha abierto nuevas vulnerabilidades y a aportado nuevas posibilidades al atacante.

2.2 Antecedentes de Investigación

Después de revisar diferentes bibliografías e investigaciones de los que he tenido acceso, tanto de Internet como de las bibliotecas especializadas, describo los trabajos más relevantes al tema de investigación, indicando que existen muy pocos trabajos relacionados directamente al tema de estudio pero si de trabajos afines referidos a las variables del presente estudio

2.2.1 Investigaciones Internacionales

En el año 2012 los investigadores Florian Kammuller, Glenford Mapp, Sandip Patel, y Abubaker Sadiq Sani de la Universidad de Londres Middlesex realizaron una investigación la cual publicaron el artículo “Protocolos de Seguridad de Ingeniería con ModelChecking - Radius-SHA256 y Secured Protocolo simple”, donde llegan a la conclusión de que El protocolo Radius utilizando SHA-256 en lugar de MD5 proporciona exactamente las mismas garantías de seguridad que la versión RFC basado en MD5.

La verificación es un análisis completamente automático en el kit de herramientas Avispa, un comprobador de modelos especializado para protocolos de seguridad. Podríamos generalizar este resultado para garantizar seguridad para los protocolos de Radius que usan funciones seguras del hash, incluso distinta de SHA-256.

En el año 2003 los investigadores Sami Keski-Kasari, Karri Huhtanen, Jarmo Harju de la Universidad Tecnológica de Tampere - Instituto de Ingeniería de Comunicaciones Finlandia publicaron el siguiente artículo “Aplicación del acceso público basado en radios en roaming” - La Red Universitaria Finlandesa (FUNET) donde llegan a la conclusión que con la función de proxy RADIUS estándar es posible llevar autenticación, autorización y contabilidad al RADIUS servidor de la universidad de origen del usuario. Porque la idea es hacer que la RADIUS servidores en diferentes universidades a parecer un gran RADIUS sistema hay una necesidad de algún tipo de jerarquía. (Huhtanen, Vatiainen, Keski-Kasari, & Harju, 2010).

Este documento describe una aplicación de esa idea y una arquitectura para llevar no sólo WLAN sino también el acceso público en general a la red FUNET y más allá.

La jerarquía se diseñará también para ser interoperable para itinerancia entre otras universidades europeas y redes universitarias, por ejemplo Como parte del grupo de trabajo sobre la movilidad de TERENA.

En el año 2015 los investigadores J.J Zhou, K. Yu y J.F. Liao de Huazhong Universidad de Ciencias y Tecnologia de Wenhua – Wuhan China publicaron el articulo : “Investigación y análisis de la era de la nube varias autenticación de red y tecnología contable” cual consideran que kerberos como un nuevo modo es adecuado para la aplicación de la autenticación de identidad del sistema de red en la nube. En muchos casos, SSO puede acceder a todo el sistema de aplicaciones de confianza mutua mediante un único acceso de banda ancha, Ethernet optimizado, protocolo IEEE 802.X + recomendando el modo de autentificación del servidor RADIUS, que puede resolver el problema de cuello de botella de los métodos tradicionales de autenticación como PPPoE y web / Portal

Dentro de las ventajas de trabajar en con esta metodología se encontraron que es una extensión de la técnica tradicional de acceso de banda estrecha PSTN en la tecnología de acceso Ethernal
Es consistente con el sistema de autenticación de acceso de red de banda estrecha original a su vez los usuarios finales son relativamente fáciles de aceptar

Dentro de las desventajas de esta metodología concluyen que El protocolo PPP tiene una diferencia esencial con la tecnología Ethernet y necesita ser encapsulado nuevamente en el marco de Ethernet, por lo que la eficiencia es muy baja. También genera una gran cantidad de tráfico de difusión en etapa Discovery que tiene un gran impacto en el rendimiento de la red

El negocio de multidifusión tiene muchas dificultades, mientras que el negocio de video se basa principalmente en multidifusión.

Exigir que los operadores proporcionen el software del terminal del cliente, la carga de trabajo de mantenimiento es excesivo

En el año 2016 los investigadores Young-Se Kim, Keun-hee Han, y Kee-Cheon Kim de la División de TI Convergencia de la seguridad de la Información de la Universidad KonKuk de Corea del Sur publicaron el siguiente articulo: “Método de autenticación mejorado del protocolo RADIUS en el entorno de Internet” cual proponen un método de autenticación del protocolo RADIUS existente analizando, el entorno IOT es más confiable que se ha investigado el cual es el método de transmisión eficiente.
Como un esquema mejorado de autenticación de paquetes en el entorno IOT a través de la comparación Orientado a mensajes y orientado a la conexión Sala de transmisión SCTP con características orientadas a la conexión.
Se encontró que la ecuación es un método de transmisión más adecuado además, al intercambiar datos entre dos objetos, la transmisión como una forma de mantener la integridad de los datos transmitidos se estudió cómo codificar la información de firma URI de un objeto.
Y En un entorno IOT donde se enfatiza la interconexión entre dispositivos, en lugar de enviar la información hash como un hash simple, se genera aleatoriamente, hay algunas formas más de mejorar la seguridad usando nonce Puede ser razonable
Utilizando el esquema de transmisión SCTP basado en el marco Diameter

En el año Febrero del 2016 el investigador Aulia Rahman & Haviluddin Universidad de Mulawarman, Kalimantan Oriental – Indonesia, publico el siguiente artículo: “Implementación de autenticación de gestión de ancho de banda”, en el cual la investigación hace referencia al mecanismo del servicio de tráfico de Internet incluye monitoreo y seguridad de la red indispensable.

Esta investigación tuvo como objetivo principal el monitoreo de red y la optimización del ancho de banda, manteniendo la seguridad de la interna de los usuarios, describiendo la implementación del Protocolo de Servicio de Usuario de Marcado de Autenticación Remota (RADIUS) y Servidor (AAA) integrado con Mikrotik cual propósito es la implementación de gestión del ancho de banda, que incluye LAN (red de área local) y Wi-Fi (fidelidad inalámbrica) en La Universidad Mulawarman. Basado en el experimento, el sistema es simple y practico de usar puesto que controla y asigna ancho de banda a los usuarios (profesores, personal y estudiantes) mientras se autentican con LAN y Wi-Fi.

El análisis de la administración de autenticación de usuario en la LAN y Wi-Fi controla y asigna usuarios de ancho de banda (profesores, personal y estudiantes). Por lo tanto, el portal cautivo es capaz de brindar comodidad al administrador para monitorear a los usuarios que acceden a Internet. Además, La perspectiva de seguridad muestra que los usuarios que no están registrados para usar Internet también podrían mantenerse.
Significa que hace que los usuarios legales visiten de manera segura todos los recursos netos del campus (LAN y Wi-Fi).

2.2.2 Investigaciones Nacionales

En el año 2015 La Ingeniera e Investigadora Rosina Gonzales Calienes de la Universidad Nacional Mayor de San Marcos Publico su investigación titulándola “Despliegue del Servicio eduroam en el Campus Universitario de la UNMSM” en esta publicación resume que el servidor RADIUS actualmente instalado en la Red Telemática es responsable de la autenticación de sus propios usuarios (locales y visitantes de otras instituciones), y del reenvío de solicitudes de usuarios visitantes al servidor RADIUS confederado Latinoamericano-LATLR, ubicado en el nodo INICTEL-UNI institución miembro de la RAAP. A nivel nacional se encuentra el servidor RADIUS de la federación (FTLR), el cual tiene una lista de servidores IdP y los dominios asociados. Este servidor FTLR recibe solicitudes de los IdP y servidores de la confederación que están conectadas, para reenviarlas desde ellos al servidor apropiado, o

en caso de una solicitud de un destino para una confederación a un servidor de la confederación.

En el año 2012 los investigadores Javier Richard Quinto Ancieta, Andres Mijail Leiva Cochachin, José Luis Quiroz Arroyo del Instituto Nacional de Investigación y Capacitación en Telecomunicaciones INICTEL realizaron una publicación la cual fue titulada “Propuesta de una infraestructura segura para el monitoreo de eventos en Eduroam Latinoamérica” donde Se analizó que los reportes actuales de eduroam Latinoamérica no permiten una gestión segura cuando de autenticarse los usuarios se trata por un determinado periodo. Esta propuesta de implementar un sistema de reportes de monitoreo para eduroam-la usando atributos del paquete freeradius y el módulo linelog del mismo. (Gonzales, 2017).

2.3 Bases Teóricas

2.3.1 Radius

La autenticación remota telefónica de servicio de usuario (RADIUS) es una red de protocolo que proporciona autenticación centralizada, autorización y contabilidad (AAA o Triple A) de gestión para los usuarios que se conectan y utilizan un servicio de red. RADIUS fue desarrollada por Livingston Enterprises, Inc. en 1991 como una autenticación de servidor de acceso Protocolo de cuentas y que posteriormente fue trasladado a las de Internet Engineering Task Force estándares (IETF). (Technet, 2017)

Debido al amplio apoyo y la naturaleza ubicua del protocolo RADIUS, a menudo es utilizado por los ISPs y las empresas para gestionar el acceso a la Internet, redes inalámbricas y servicios de correo electrónico integrado. Estas redes pueden incorporar los módems, DSL, puntos de acceso, VPNs , puertos de red , servidores web , etc.

RADIUS es un protocolo cliente/servidor que se ejecuta en la capa de aplicación, y se puede utilizar ya sea TCP o UDP como transporte. Servidores de acceso a la red, las puertas de enlace que controlan el acceso a una red, por lo general contienen un componente de cliente RADIUS que se comunica con el servidor RADIUS. RADIUS es a menudo el back-end de elección para 802.1X autenticación también.

El servidor RADIUS es generalmente un proceso en segundo plano que se ejecuta en un servidor UNIX o Microsoft Windows

2.3.1.1 AAA. En seguridad informática, AAA significa comúnmente autenticación, autorización y contabilidad. Se refiere a una arquitectura de seguridad para sistemas distribuidos que permite control sobre qué usuarios se les permite el acceso a qué servicios y que mantiene las pestañas en cuánto de los recursos que han utilizado. Dos protocolos de red que proporcionan este son particularmente populares: el protocolo RADIUS y su nuevo diámetro contrapartida.

2.3.1.2 Autenticación. Usaremos el protocolo EAP, el cual consiste en mensajes de solicitud y respuesta entre el suplicante, el autenticador y el servidor de autenticación RADIUS de la organización de origen a la cual pertenece el usuario.

En el escenario que el usuario requiera autenticarse desde otra organización de la cual no es su organización de origen, las solicitudes y respuestas de mensajes pasaran por los autenticadores de la organización visitante hasta el servidor de origen del usuario, y a su vez estarán incluidos los servidores Proxy RADIUS que interconecten.

Observamos distintos tipos de mecanismos de autenticación que utilizan EAP, por lo que estos pueden ser clasificados en dos categorías:

- La primera categoría utiliza mensajes que son enviados desde el cliente hasta el servidor RADIUS de origen vía una cadena de servidores RADIUS sin estar cifrados. Para este caso el protocolo es vulnerado por ataques de Man-In-The-Middle, y esto podría comprometer en algún punto de la cadena de servidores RADIUS.

La segunda categoría utiliza el protocolo EAP basada en la autenticación de conexiones TLS. (TELEM@TICA, 2015)

En el caso de la confederación eduroam requiere y es una necesidad el intercambio seguro de credenciales con una autenticación segura, por ello

los mecanismos que expongan las credenciales sin usar cifrado en los servidores intermedios es prohibida.

2.3.1.3 Autorización. Normalmente significa que un subconjunto de los atributos asociados a un usuario coincide con los requisitos del servicio al que se debe acceder. El resultado de verificar la autorización de una persona es Aceptar o rechazar el acceso y, posiblemente, asignar al usuario a un nivel de servicio específico.

La verificación de la autorización en Eduroam tiene lugar en dos fases:

- En primer lugar, se determina el nivel de servicio deseado en función de los atributos contenidos en la solicitud de acceso
- En segundo lugar, se establecen los niveles de servicio adecuados para la sesión del usuario.

Rechazar el acceso El usuario se le deniega el acceso sin condiciones a todos los recursos de la red solicitados. Las razones pueden incluir la imposibilidad de presentar pruebas de identificación o una cuenta de usuario desconocido o inactivo.

El acceso Challenge Las solicitudes de información adicional por parte del usuario como la contraseña secundaria, PIN, token o tarjeta. El acceso Challenge también se utiliza en los cuadros de diálogo de autenticación más compleja en las que se establece un túnel seguro entre el equipo de usuario y el servidor RADIUS de una manera que las credenciales de acceso se ocultan de la NAS.

Acceso Aceptar Se otorga al usuario el acceso. Una vez autenticado el usuario, el servidor RADIUS a menudo comprobar que el usuario está autorizado a utilizar el servicio solicitado. Un usuario dado puede ser permitido el uso de la red inalámbrica de una empresa, pero no su servicio VPN, por ejemplo. Una vez más, esta información puede ser almacenada

localmente en el servidor RADIUS, o puede ser consultada en un dispositivo externo como LDAP o Active Directory.

Cada una de estas tres respuestas RADIUS puede incluir un atributo Responder-mensaje que puede dar una razón para el rechazo, el símbolo para el desafío, o un mensaje de bienvenida para la acepte. El texto en el atributo puede ser transmitido al usuario en una página web de retorno.

De autorización atributos se transportan a los NAS que estipulan términos de acceso a determinados. Por ejemplo, los siguientes atributos de autorización pueden ser incluidos en una de aceptación de acceso:

- La específica dirección IP que se debe asignar al usuario
- El conjunto de direcciones a partir del cual se debe elegir IP del usuario
- La longitud máxima de tiempo que el usuario puede permanecer conectado
- Una lista de acceso, cola de prioridad u otras restricciones sobre el acceso de un usuario
- L2TP parámetros
- los parámetros de VLAN
- Parámetros de calidad de servicio (QoS). (Cisco, 2006)

Cuando un cliente está configurado para utilizar RADIUS, cualquier usuario del cliente presenta información de autenticación al cliente. Esto podría ser un inicio de sesión personalizable, donde se espera que el usuario introduzca su nombre de usuario y contraseña. Alternativamente, el usuario puede utilizar un protocolo de enlace de enmarcar tales como el Punto-a-Punto (PPP), que tiene los paquetes de autenticación que llevan esta información.

Una vez que el cliente ha obtenido dicha información, se puede optar por la autenticación mediante RADIUS. Para ello, el cliente crea una "Solicitud

Cómo acceder" contiene atributos tales como el nombre del usuario, la contraseña del usuario, el ID del cliente y el ID de puerto que el usuario está accediendo. Cuando una contraseña está presente, se oculta utilizando un método basado en el RSA Message Digest MD5 algoritmo.

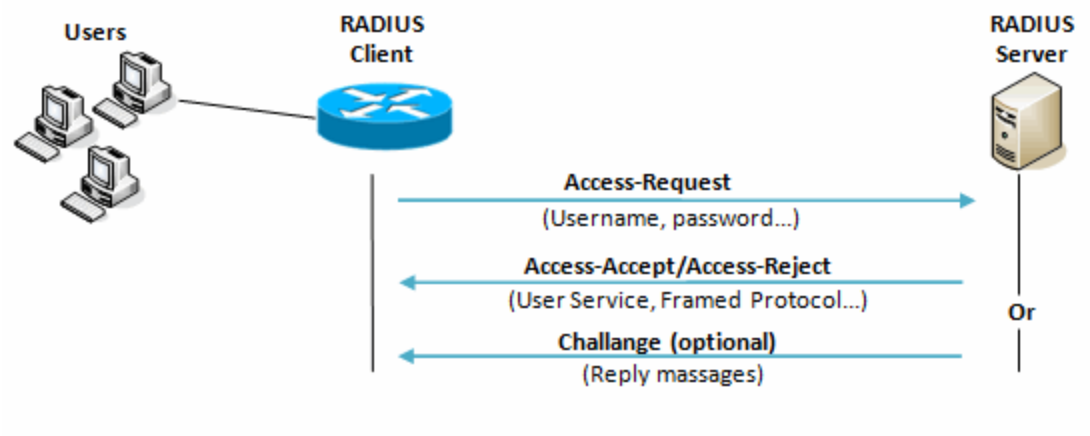


Figura 1. **Flujo de Autorización y Autenticación en RADIUS.**

Fuente: Documentación Microtik

2.3.1.4 Administración. Cuando el acceso a la red se concede al usuario por el NAS, al inicio de la Contabilización (un paquete de petición de cuentas RADIUS que contiene un atributo Acct-Status-Type con el valor "start") es enviado por el NAS en el servidor RADIUS para señalar el comienzo de acceso a la red del usuario. "Inicio" registros suelen contener la identificación del usuario, dirección de red, punto de unión y un identificador de sesión único.

Periódicamente, actualización provisional registros (un paquete de petición de cuentas RADIUS que contiene un atributo Acct-Status-Type con el valor "provisional de actualización") pueden ser enviados por el NAS al servidor RADIUS, para actualizarlo sobre el estado de una sesión activa. Registros "provisionales" por lo general transmiten la duración de la sesión actual y la información sobre el uso de datos actual.

Por último, cuando el acceso a la red del usuario se cierra, el NAS emite una final de Contabilidad Detener registro (un paquete de Solicitud de Contabilidad RADIUS que contiene un atributo Acct-Status-Type con el valor de "parada") al servidor RADIUS, que proporciona información sobre el uso final de en términos de tiempo, los paquetes transferidos, los datos transferidos, razón por la desconexión y otra información relacionada con el acceso a la red del usuario.

Normalmente, el cliente envía paquetes de Contabilidad-Solicitud hasta que recibe un acuse de recibo de Contabilidad-Respuesta, usando un intervalo de reintento.

El propósito principal de estos datos es que el usuario puede ser facturado en consecuencia; los datos también se utilizan comúnmente para estadísticos propósitos y para la monitorización de la red general.

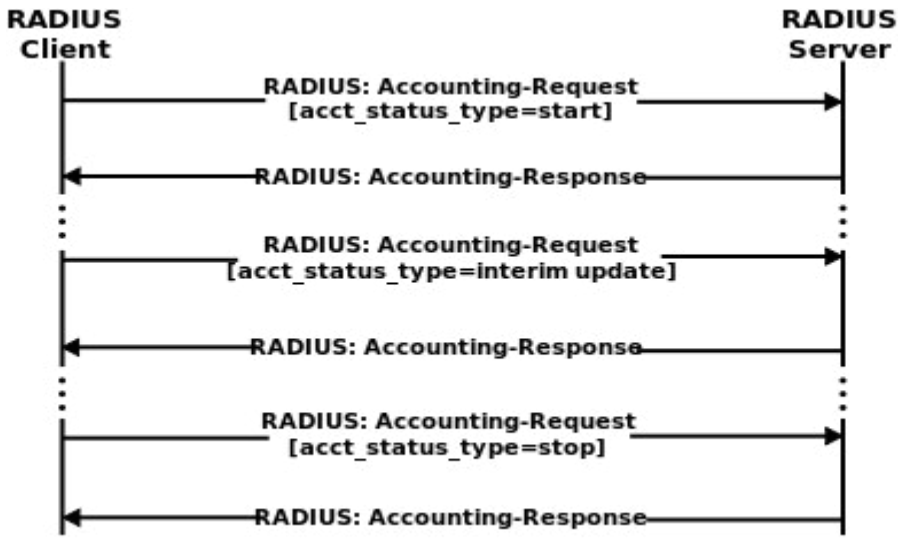


Figura 2: **Flujo de Contabilidad.**

Fuente: Wikipedia

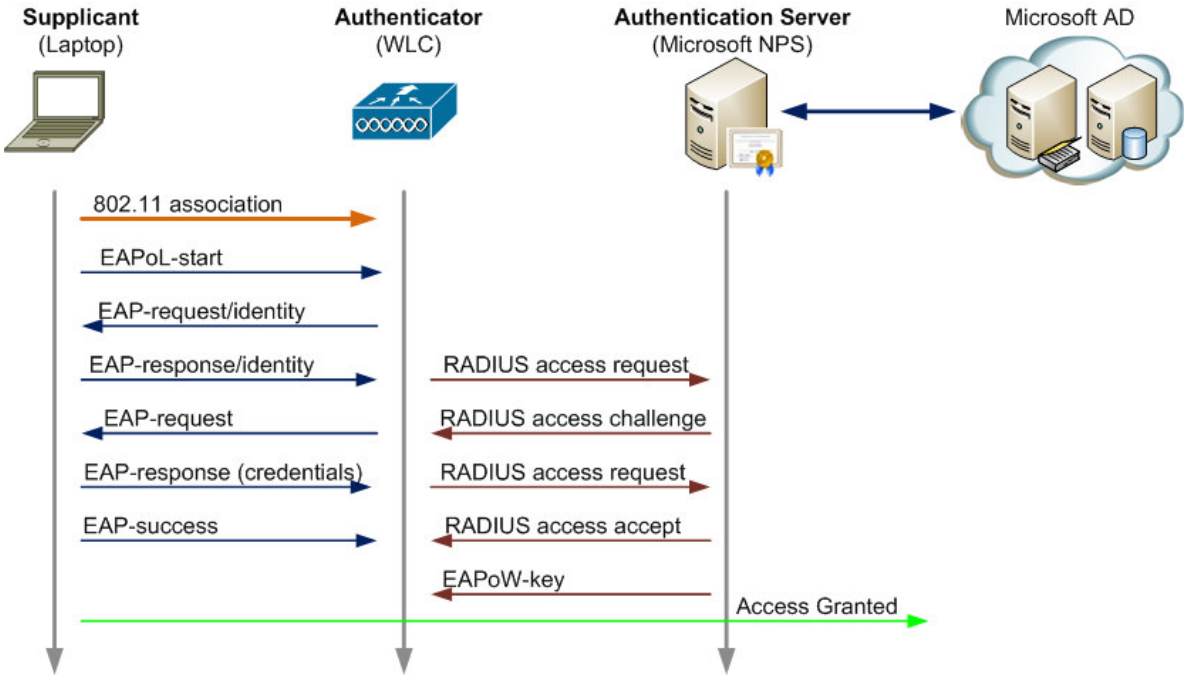


Figura 3: **Intercambio de autenticación 802.1x**

Fuente: http://bowdennetworks.co.uk/

2.3.1.5 Itinerancia o roaming. RADIUS se utiliza comúnmente para facilitar la itinerancia entre los proveedores de Internet, por ejemplo: las empresas que proporcionan un único conjunto global de las credenciales que se pueden utilizar en muchas redes públicas; por independientes, sino colaborar, instituciones que emiten sus propias credenciales para sus propios usuarios, que permiten que el visitante de una a otra para ser autenticados por su institución de origen, como en eduroam. (Cisco, 2006)

RADIUS facilita esto mediante el uso de reinos, que identifican donde el servidor RADIUS debe remitir las solicitudes AAA para su procesamiento.

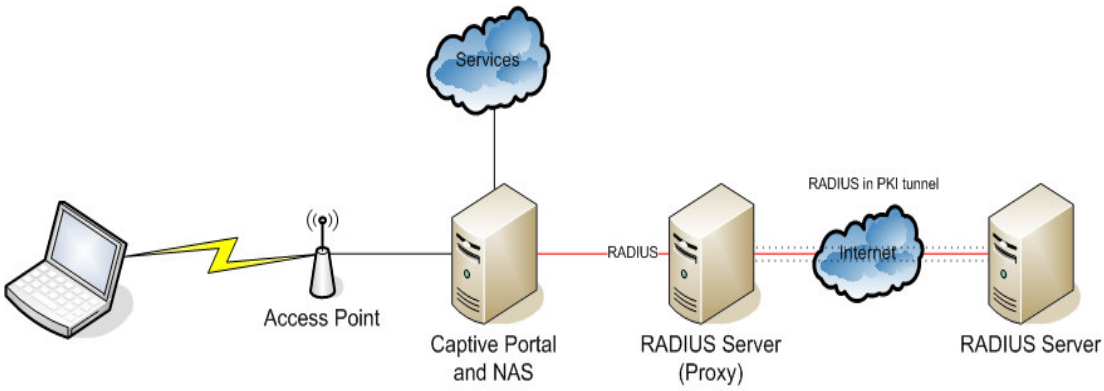


Figura 4: **Roaming utilizando un servidor proxy RADIUS AAA.**

Fuente. wiki/RADIUS

2.3.1.6 Realms. Un Realms se añade comúnmente para el nombre de usuario de un usuario y delimitado con un signo "@", se asemeja a un nombre de dominio dirección de correo electrónico. Esto se conoce como postfix otación para el reino. Otro uso común es el prefijo de notación, que consiste en anteponer el reino al nombre de usuario y usando '\' como delimitador. Los servidores RADIUS modernos permiten que cualquier carácter que se utiliza como un delimitador de campo, aunque en la práctica '@' y '\' se utilizan normalmente. (Wikipedia, 2017)

Realms también se pueden componer utilizando tanto la notación de prefijo y postfijo, para permitir la itinerancia escenarios complicados; por ejemplo, somedomain.com \ username@anotherdomain.com podría ser un nombre de usuario válido con dos reinos.

Aunque Realms menudo se asemejan a dominios, es importante tener en cuenta que Realms son, de hecho, texto arbitrario y no necesita contener nombres de dominio reales. Realm formatos están estandarizados en el RFC 4282, que define una Red de Acceso Identificador (NAI) en forma de "usuario @ dominio". En esa memoria descriptiva, se requiere la porción de ´Realm´ ser un nombre de dominio. Sin embargo, esta práctica no siempre es seguida. RFC 7542 sustituye RFC 4282 en de mayo de 2015.

2.3.1.7 Proxy Operations. Cuando un servidor RADIUS recibe una solicitud de AAA para un nombre de usuario que contiene un dominio, el servidor hará referencia a una tabla de dominios configurados. Si se conoce el reino, el servidor entonces proxy de la solicitud al servidor de red configurada para ese dominio. El comportamiento del servidor proxy con respecto a la eliminación de la esfera de la solicitud ("stripping") es de configuración dependiente en la mayoría de los servidores. Además, el servidor proxy se puede configurar para añadir, eliminar o reescribir solicitudes AAA cuando están proxy en el tiempo de nuevo.

El encadenamiento de proxy es posible en los paquetes RADIUS y autenticación / autorización y contabilidad se dirige generalmente a entre un dispositivo NAS y un servidor principal a través de una serie de servidores proxy. Algunas de las ventajas de la utilización de cadenas de proxy incluyen mejoras de escalabilidad, las implementaciones de políticas y los ajustes de capacidad. Pero en itinerancia escenarios, el NAS, servidores proxy y servidor principal se podrían normalmente gestionados por diferentes entidades administrativas. Por lo tanto, el factor de la confianza entre los proxies adquiere más importancia en tales aplicaciones inter-dominio. Además, la ausencia de un extremo a otro de la seguridad en RADIUS se suma a la criticidad de la confianza entre los proxies implicados. Cadenas de proxy se explican en el RFC 2607.

2.3.1.8 Seguridad. Itinerancia con RADIUS expone a los usuarios a diversas preocupaciones de seguridad y privacidad. En términos más generales, algunos socios de roaming establecen un túnel seguro entre los servidores RADIUS para asegurar que las credenciales de los usuarios no pueden ser interceptados mientras se proxy a través de Internet. Esta es una preocupación que la suma MD5 integrado en RADIUS se considera inseguro. (Wikipedia, 2017)

2.3.1.9 Estructura de paquetes. El formato de paquete de datos RADIUS se muestra a la derecha. Los campos se transmiten de izquierda a derecha, empezando por el código, el identificador, la longitud, el autenticador y los atributos.

Códigos de radio (decimales) se asignan de la siguiente forma

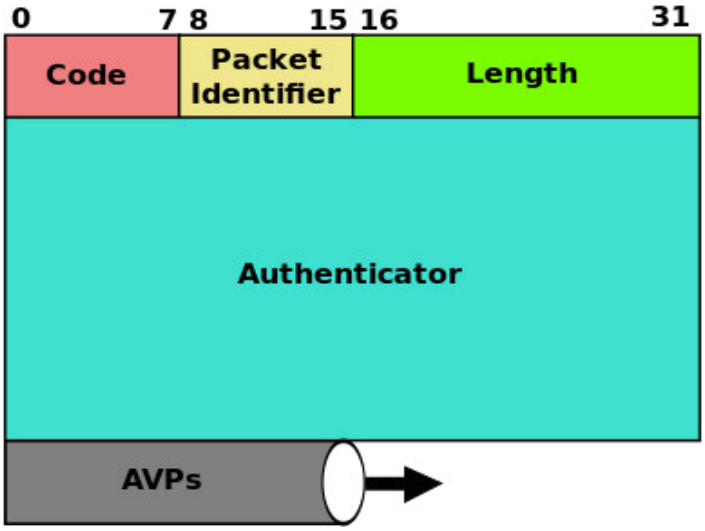


Figura 5: **Formato de paquete RADIUS.**

Fuente Wiki Radius

2.3.2 Ldap (Lightweight Directory Access Protocol)

Es un protocolo de software que permite a cualquier persona localizar organizaciones, individuos y otros recursos, como archivos y dispositivos en una red, ya sea en la Internet pública o en una intranet corporativa. LDAP es una versión "ligera" (menor cantidad de código) del Protocolo de acceso a directorios (DAP), que forma parte de X.500, un estándar para servicios de directorio en una red. LDAP es más ligero porque en su versión inicial no incluía características de seguridad. LDAP se originó en la Universidad de Michigan y ha sido aprobado por al menos 40 empresas. Netscape lo incluye en su último conjunto de productos Communicator. Microsoft lo incluye como

parte de lo que llama Active Directory en una serie de productos, incluyendo Outlook Express. Los servicios de directorio NetWare de Novell interactúan con LDAP. Cisco también lo admite en sus productos de red.(what-when-how, 2017)

En una red, un directorio le dice dónde se encuentra en la red algo. En las redes TCP / IP (incluido Internet), el sistema de nombres de dominio (DNS) es el sistema de directorios utilizado para relacionar el nombre de dominio con una dirección de red específica (una ubicación única en la red). Sin embargo, es posible que no conozca el nombre de dominio. LDAP le permite buscar un individuo sin saber dónde están ubicados (aunque información adicional ayudará con la búsqueda).

Un directorio LDAP está organizado en una simple jerarquía "árbol" que consta de los siguientes niveles:

- El directorio raíz (el lugar de inicio o el origen del árbol), que se ramifica a Países, cada uno de los cuales Las organizaciones, que se son Unidades de organización (divisiones, departamentos, etc.), que se ramifica a (incluye una entrada para)
- Los individuos (que incluyen personas, archivos y recursos compartidos, como impresoras)

Un directorio LDAP se puede distribuir entre muchos servidores. Cada servidor puede tener una versión replicada del directorio total que se sincroniza periódicamente. Un servidor LDAP se denomina DSA (Directory System Agent). Un servidor LDAP que recibe una solicitud de un usuario asume la responsabilidad de la solicitud, pasándola a otros DSA según sea necesario, pero garantizando una única respuesta coordinada para el usuario.

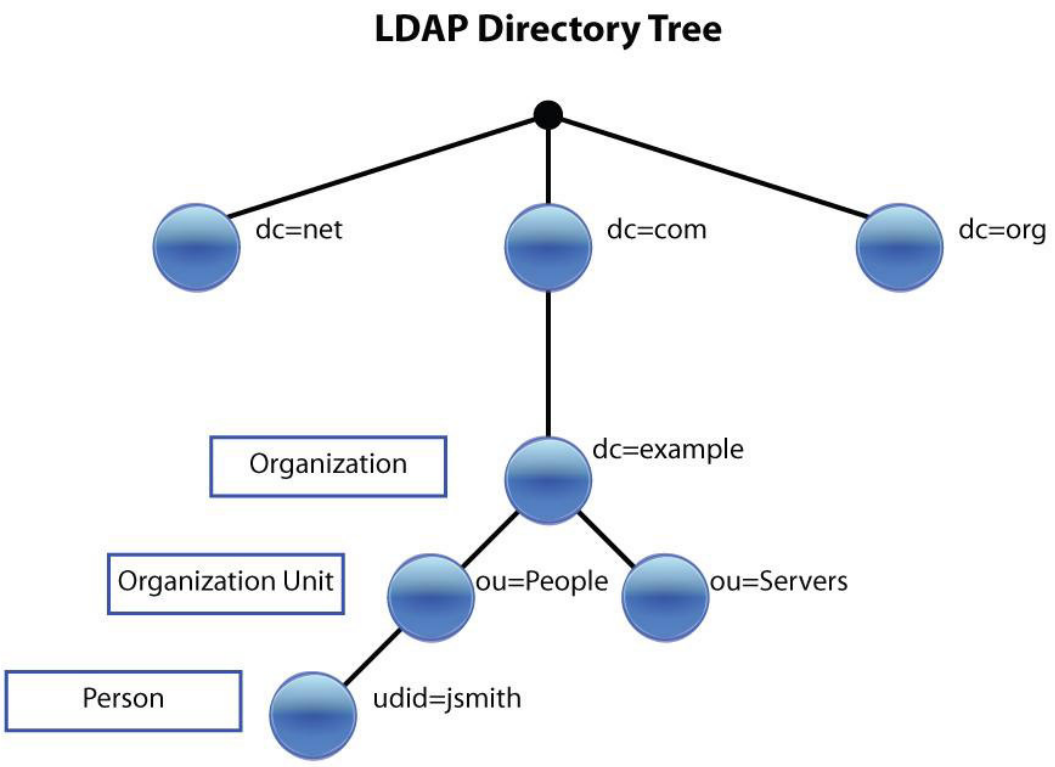


Figura 6: **Árbol de directorios.**

Fuente: Balanceo de Carga - Craig Thomas Ellrod

2.3.3 IEEE 802.11X

El estándar 802.1X está diseñado para mejorar la seguridad de las redes WLANs. Por otro lado provee una autenticación para redes LAN, permitiendo al suplicante/usuario autenticarse por una autoridad central. (Searchmobilecomputing, 2017)

802.1X requiere del protocolo EAP (Extensible Authentication Protocol) el cual también está implicado en los procesos de WLANs, Token Ring, Ethernet para el intercambio de mensajes durante el proceso de autenticación. Este protocolo EAP transporta los datos de autenticación a través de EAPol y dentro del protocolo RADIUS.

En este proceso el Autenticador que viene hacer el NAS (Punto de acceso Inalámbrico o conmutador) que verificara el estado y la designación de

pertenencia a la VLAN que corresponda en caso se conecte con el suplicante.

Durante este proceso los mensajes de autenticación y autorización es realizada por el solicitante y el servidor de Autenticación, por lo tanto el servidor enviaría un paquete de “Aceptación” o “Rechazo” del autenticador, permitiendo o rechazando al usuario, como consecuencia de la respuesta del Servidor de Autenticación el autenticador mantendrá o cerrara el puerto sea el caso.

El uso versátil de 802.1X para diferentes métodos de autenticación son usados dentro de EAP, EAP-MD5, EAP-OTP (One-Time Password), EAP-GTC (Generic Token Card) y EAP-SIM como ejemplos. Es relevante conocer la confianza del Servidor de Autenticación para el suplicante previo el envió de información sensible como el usuario y contraseña. Por ello el cliente tiene la opción de verificar el certificado con una copia instalada de la clave pública de la entidad emisora de certificados (CA) y una lista de certificados revocados (CRL) antes de proseguir con el proceso de autenticación.

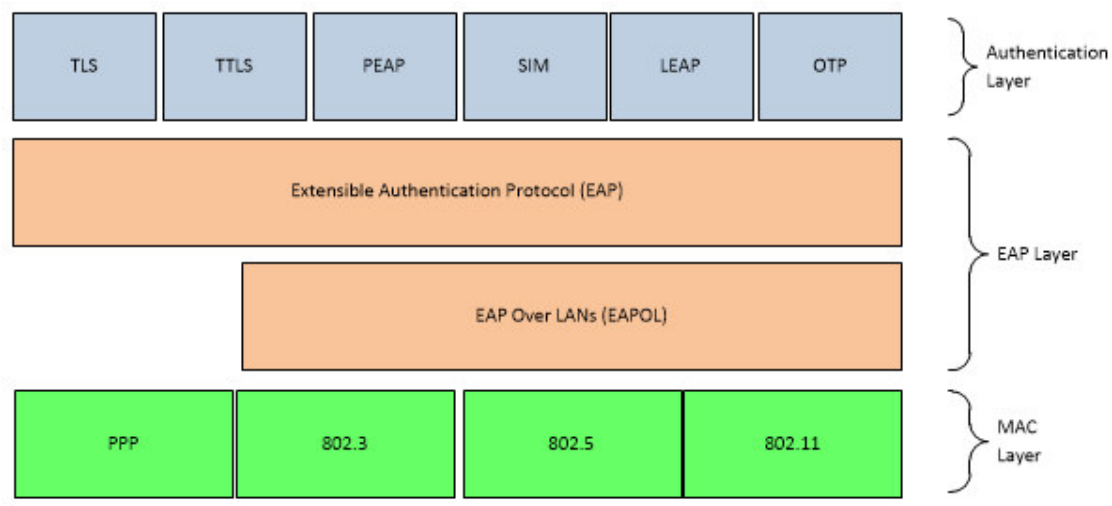


Figura 7: ***Las capas de autenticación EAP***

Fuente: Autor de Tesis

2.3.4 NAS (Network Access Server)

Un NAS concentra marcación de entrada y de acceso telefónico a cabo las comunicaciones del usuario. Un servidor de acceso puede tener una mezcla de las interfaces analógicas y digitales y apoyar a cientos de usuarios simultáneos. Un NAS consiste en un procesador de comunicaciones que conecta dispositivos asíncronos a una red LAN o WAN a través de la red y de emulación de terminal de software. Se lleva a cabo el enrutamiento síncrona y asíncrona de los protocolos soportados.

El NAS está destinado a actuar como una puerta de enlace para proteger el acceso a un recurso protegido. Esto puede ser cualquier cosa desde un teléfono de la red , a las impresoras , a la Internet . Un cliente se conecta a la NAS. El NAS se conecta a otro recurso preguntan si suministradas por el cliente credenciales son válidas. En base a esa respuesta el NAS a continuación, permite o prohíbe el acceso al recurso protegido. (Revolvy, 2017).

2.3.5 EAP (Extensible Authentication Protocol)

Es una autenticación de marco utilizado con frecuencia en las redes inalámbricas y conexiones de punto a punto. Se define en RFC 3748, lo que hizo RFC 2284 obsoleta, y se actualiza por RFC 5247.

EAP es un marco de autenticación para proporcionar el transporte y el uso de materiales y parámetros de claves generado por métodos EAP. Hay muchos métodos definidos por RFC y un número de proveedor existen métodos específicos y nuevas propuestas. EAP no es un protocolo de conexión; en vez de eso sólo define los formatos de mensaje. Cada protocolo que utiliza EAP define una forma de encapsular los mensajes EAP dentro de los mensajes de ese protocolo. (Tecnología hecha palabra, (2007).

EAP es de amplio uso. Por ejemplo, en IEEE 802.11 (Wi-Fi) de la WPA y WPA2 han adoptado normas IEEE 802.1X con cien tipos de EAP como los mecanismos oficiales de autenticación.

El servicio eduroam utiliza tres tipos de EAP para su despliegue. Estos procesos otorgan la autenticación de cifrado mutua entre suplicante y el servidor de autenticación.

Se indica también que no todos los servidores RADIUS o suplicantes soportan estos tres tipos de EAP, pese a ello el servidor RADIUS puede soportar dos tipos de EAP, y esto se puede usar simultáneamente a la configuración del suplicante.

2.3.5.1 EAP – TLS. (Transport Layer Security) trabaja con el uso de los certificados para la autenticación entre el servidor y el suplicante. Este proceso se inicia cuando el servidor envía su certificado el cual contiene su llave pública al cliente. A continuación el cliente verifica la llave con un apropiado certificado de autorización (CA). Por lo tanto si la verificación de las llaves no presenta error y cumple con los parámetros establecidos, el cliente envía su propio certificado que contiene una clave pública al servidor de autenticación. Como consecuencia el servidor de autenticación revisara la llave publica y si es validada la autenticación será exitosa.

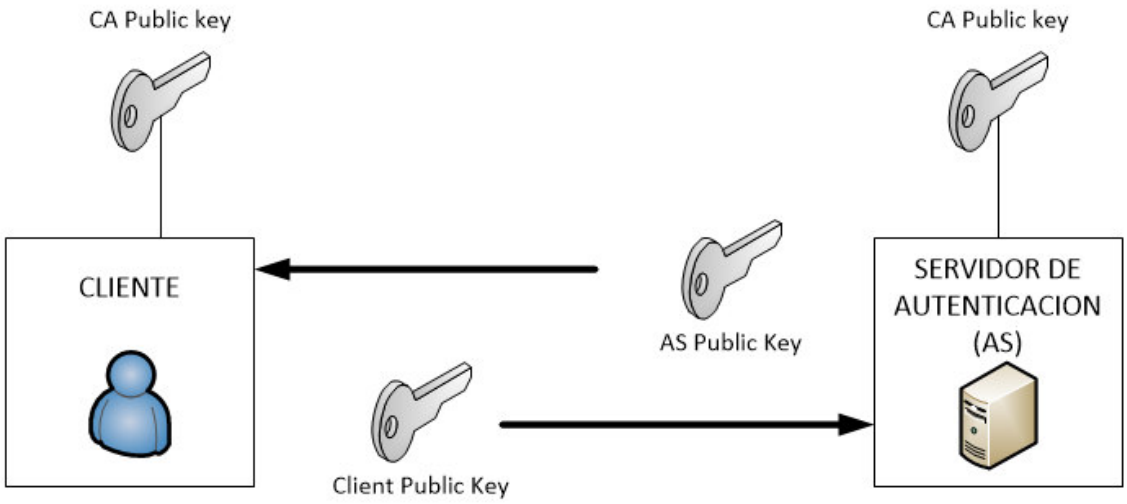


Figura 8: ***Uso de PKI en EAP-TLS***

Fuente: Autor de Tesis

2.3.5.2 EAP – TTLS. El protocolo TTLS establece un túnel de seguridad entre el servidor de autenticación y el suplicante, del mismo modo en la autenticación de EAP-TLS, para este caso también se envía una llave publica al cliente desde el servidor de autenticación, quien luego verificara esta llave pública. Una vez realizada la autenticación del servidor, el suplicante utiliza un protocolo de autenticación basados en contraseña como PAP, CHAP o MS-CHAP. Estas contraseñas se transfieren en el túnel TLS con atributos de DIAMETER. Cabe mencionar que el protocolo con mayor uso dentro de TTLS es el PAP. Sea el caso siempre requerirá las credenciales válidas para la autenticación. (Cisco, 2017)

2.3.5.3 EAP – PEAP. PEAP No es un protocolo de cifrado como los otros tipos de EAP, la diferencia es que para la autenticación de los clientes solo utiliza certificados de clave pública del lado del servidor, creando así un túnel SSL/TLS cifrado entre el Servidor de autenticación y cliente.

Este protocolo es muy similar al EAP-TTLS debido a que solo requiere un certificado PKI del lado del servidor para crear el túnel TLS seguro y proteger la autenticación del cliente.

En la práctica solo se utiliza el protocolo de autenticación interna que es el EAP-MS-CHAPv2.

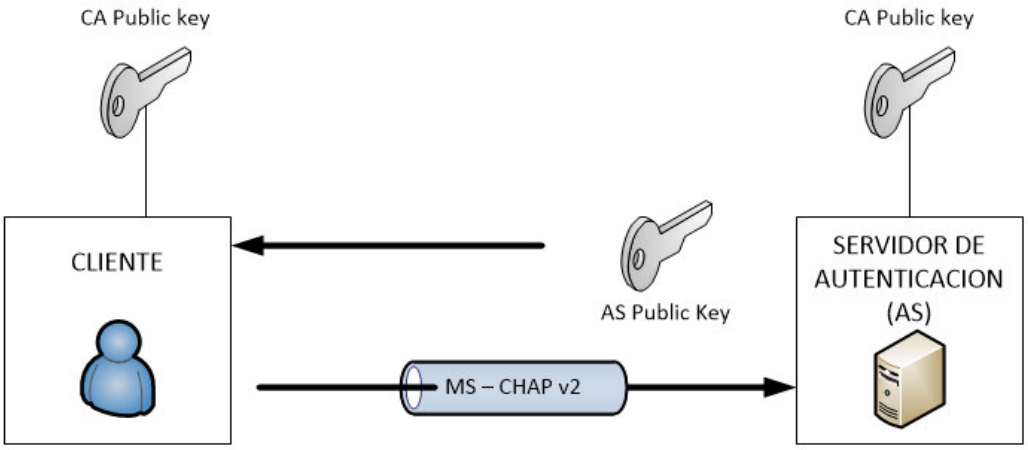


Figura 9: **PKI and MS-CHAPv2 within PEAP**

Fuente: Autor de Tesis

2.3.6 Eduroam

El concepto de eduroam es la contracción de educación por roaming es un servicio mundial de itinerancia para la comunidad de investigadores internacionales. Iniciándose en Europa logro impulsar a través de la comunidad de investigación y educación por lo que actualmente se encuentra en 72 territorios. Este servicio permite a los estudiantes, investigadores y equipos de participantes instituciones acceder a la conexión de internet a través del campus de la Institución visitante con el lema de "Abre tu portátil y estas conectado"

Este servicio se encuentra habilitado en cientos de localidades a través de 70 países a nivel mundial, específicamente en universidades e instituciones de investigación. La Forma de trabajo del servicio eduroam permite que los usuarios conectados logren acceder a las institución que brindan este

servicio las cuales se encuentran conectadas a nivel mundial como una sola red. Depende de las políticas de cada institución el acceso a sus servicios internos para cada visitante que requiera el servicio.

Las credenciales de los usuarios se mantienen seguras debido a que eduroam no las comparte en las instituciones visitantes, sino que son reenviadas a la institución de origen para ser validadas y verificadas.

El sistema usa una red de servidores, por los que los participantes que componen esta red son las Redes nacionales de Investigacion y educación – (NRENs National Research and Education Networks)

2.3.6.1 Componentes y protocolos. Se indica a continuación los siguientes elementos.

- Network Access Server (NAS): Corresponde a un equipo conmutador o un punto de acceso inalámbrico (AP) el cual proporcionara acceso a la red local.
- Client/ Supplicant – Dispositivo final del usuario para su autenticación en el acceso a la red local
- Authentication Servers (AS) – Cumple la función de autenticación y autorización de los suplicantes. Utiliza una base de datos donde se encuentran las credenciales de los usuarios (contraseñas y certificados)
- IEEE 802.1X [1X] – Estándar para el control de acceso de red basado en puertos.
- IEEE 802.1Q [1Q] – Estándar para la asignación de VLAN**.**

2.3.6.2 Servidores de Autenticación RADIUS: *E*s un protocolo cliente/servidor que trabaja entre un NAS (Servidor de acceso de red) y un AS (Servidor de Autenticación). El servidor RADIUS trasmite mensajes de autenticación, autorización contabilidad y configuración.

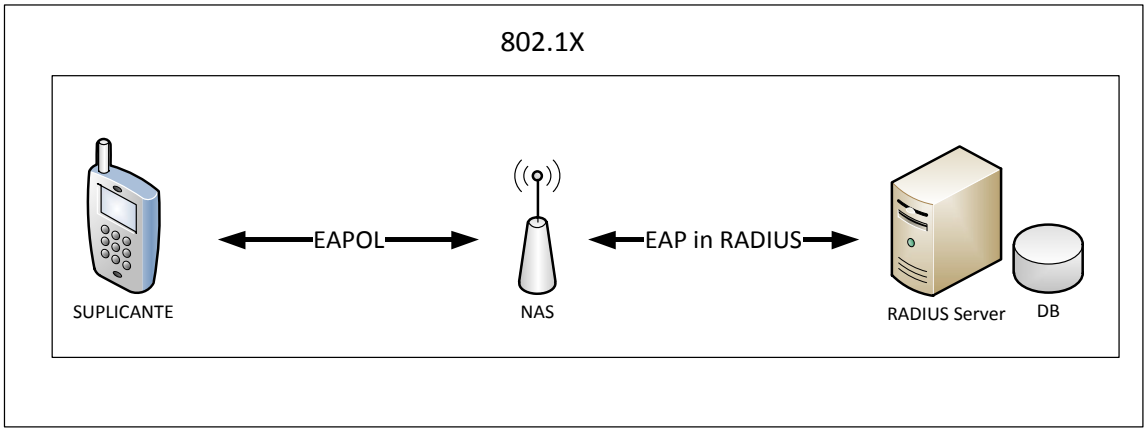


Figura 10: **IEEE 802.1X Interacciones entre componentes**

Fuente: Autor de Tesis

El cliente usa un suplicante para conectarse con el NAS y solicita un acceso a la red. La función del NAS es el control de acceso a la red. Entre el suplicante y el NAS utiliza el protocolo EAPoL.

El NAS encapsula la carga útil del EAP y transporta la autenticación del mensaje hacia el servidor RADIUS. El servidor RADIUS verifica la autenticación, la cual opta por aceptar o rechazar la solicitud de acceso. El NAS actúa en consecuencia de la respuesta del Servidor RADIUS, negando o permitiendo el acceso de la red al cliente.

El Servidor de Autenticación utiliza diversos métodos de autenticación, dependiendo de la implementación tales como, archivos de texto, Base de datos SQL, Certificados de Autorización y Bases de Datos LDAP, son ejemplos de fuentes de credenciales que los Servidores de Autenticación pueden verificar y validar la identidad del usuario. El uso de algunos métodos en combinación con otros criterios tales como prefijos y sufijos al nombre de usuario, la identidad del NAS solicitante etc.

Dentro de las configuraciones en el servidor RADIUS también es posible optar para una configuración en el NAS de modo que se controle la asignación por VLANs, esto permitirá utilizar diferentes criterios según la VLAN a la cual sea asignado el usuario.

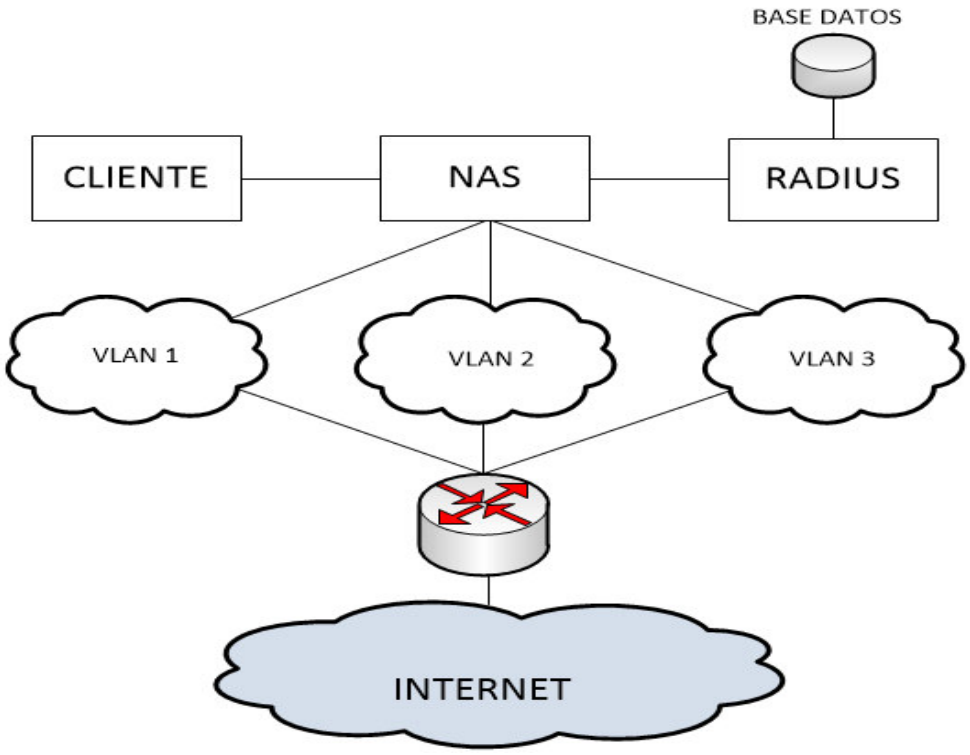


Figura 11: Asignación en diferentes VLANs por el dispositivo NAS

Fuente: Autor de Tesis

2.3.6.3 Modos de Operación. Examinamos la infraestructura desde una perspectiva orientada al servicio

- Entidades de autenticación que deseen eduroam (Servicio de autenticación)
- Encontrar un Proveedor de Identidad (IdP - Identity Provider) con información autorizada sobre la entidad (Home Location Service)
- Intercambiar atributos que describen la entidad (Servicio de Intercambio de Atributos)
- Determinar qué nivel de servicio la entidad está autorizada a utilizar (Servicio de Autorización)

2.3.6.4 Localización del servidor de origen. Son necesarios los procesos de autenticación y autorización, para localizar al servidor de origen de la organización a la que pertenece el usuario.

El servicio eduroam, se basa en dos funciones otorgadas por los servidores RADIUS que comprenden la jerarquía RADIUS de eduroam de este modo

- La primera es con el funcionamiento del proxy el cual otorga al servidor RADIUS que pasen los mensajes RADIUS hacia distintos servidores RADIUS (se considera cualquier protocolo encapsulado como el EAP)
- La segunda función está basada en la decisión de los REALM que son los nombres de usuario presentado internamente en los paquetes RADIUS. Para este caso eduroam el dominio se basa en el mismo dominio DNS de la identidad del usuario.

La ventaja de estas dos funciones es permitir a los servidores RADIUS de eduroam el localizar al servidor RADIUS de la organización de origen estableciendo una conexión virtual entre servidor y cliente.
Ambas funciones permiten localizar al servidor RADIUS de la organización del cliente.

2.3.6.5 Intercambio de atributos. La arquitectura basada en el protocolo RADIUS y los mensajes que proporciona el intercambio de atributos está limitado por las capacidades de RADIUS. Existe un numero de atributos predefinidos para RADIUS de IETF, tales como dirección MAC con lo cual el usuario intentara autenticarse.

El número de atributos está definido y limitado por 256 y esta se encuentra reglamentada por la IANA. Es de conocimiento los mecanismos que permiten a RADIUS el transporte arbitrario de atributos. Usar los atributos RADIUS ya sea en modo oficial o no tiene sus deficiencias. Por ello lo más resaltante es que no hay un estándar en el modo cifrado de contenidos para trasmitir los atributos extremo –extremo ó end-to-end. Últimamente algunos proveedores han desarrollado de extensiones patentadas para RADIUS que permiten conexiones seguras end-to-end para atributos específicos del

proveedor, usar estos atributos patentados por algún proveedor no es una opción para eduroam.

Otra deficiencia que apreciables es que el protocolo RADIUS tiene limitada capacidades de negociación donde los atributos debieran ser transportados.

Por ello eduroam solo utiliza los atributos dados de manera oficial por la IANA.

2.3.6.6 Determinación del nivel de servicio deseado. Como ya se mencionó, la autorización de los atributos están limitados por las condiciones brindadas por el servidor RADIUS de la Institutcion donde el usuario intenta acceder.

Por ello una verificación inmediata es determinar si el acceso es brindado a un invitado o a un usuario perteneciente a la institución y esto se determina por el realm o los atributos del nombre del usuario.

La comprobación más obvia es si el usuario es un invitado o si pertenece a la institución local. Esto puede determinarse fácilmente examinando el dominio del usuario, ya que el atributo real del atributo User-Name del paquete RADIUS es siempre el correcto (en contraposición a la parte local del nombre de usuario, que puede estar oscurecida en varios EAP Tipos). Estos realm´s también se pueden utilizar para definir conjuntos específicos de privilegios que se conceden a los usuarios (este nivel de privilegio puede ser mayor o menor en comparación con invitados de otros realm´s).

Otro método para determinar el nivel de servicio es examinar el protocolo de autenticación que el usuario está usando para autenticar. La razón de tal verificación es asegurarse de que los usuarios han configurado correctamente sus suplicantes, de modo que sólo transportan credenciales de una manera que se considera segura. Esto se puede lograr inspeccionando el contenido de la solicitud de autenticación. Cuando se utiliza uno de los tipos de autenticación RADIUS que no utilizan el atributo

EAP-Message, la distinción entre mecanismos es bastante trivial, ya que los tipos de atributos RADIUS que se suministran difieren entre mecanismos. Cuando se utiliza EAP-Message, la distinción es un poco más difícil, pero también se puede hacer mirando los primeros bytes del paquete EAP para averiguar sobre su EAPType. Esta es una característica que está disponible en la mayoría de los servidores RADIUS actuales.

De forma limitada, el nivel de autorización de un usuario también puede depender de la ubicación que está visitando actualmente. Sólo se puede obtener un control aproximado sobre la ubicación del usuario debido a la naturaleza del protocolo RADIUS. Los niveles actuales de separación son:

- El usuario sólo puede acceder a la red en su organización de origen (sin roaming). Los intentos de iniciar sesión desde una ubicación no autorizada pueden detectarse comprobando si la solicitud de autenticación se reenvía desde el servidor RADIUS eduroam a nivel de federación.
- El usuario puede moverse dentro de la federación, pero no en el extranjero (roaming nacional). Los intentos de iniciar sesión desde una ubicación no autorizada pueden detectarse comprobando si la solicitud de autenticación se reenvía desde el servidor RADIUS de la confederación europea eduroam. Esta configuración puede utilizarse, por ejemplo, cuando los grupos de usuarios como los alumnos deban restringirse únicamente al acceso de roaming nacional.
- Todas las ubicaciones están permitidas para el usuario. En este caso, no se necesitan revisiones de ubicación.
- Un control más fino sobre la ubicación del usuario podría lograrse si los servidores RADIUS a nivel de institución esvieran obligados a transportar una información de ubicación dentro del paquete RADIUS Access-Request, por ejemplo con las extensiones RADIUS [GeoPriv] del grupo de trabajo IETF Geopriv. Está en una fase inicial de desarrollo y no trivial de implementar.

CAPITULO 3: METODOLOGÍA

3.1 Hipótesis general

El Desarrollo e Implementación de un Sistema de Seguridad de Control de Acceso con RADIUS produce efectos que determina el grado de autenticación y autorización en el control de tráfico inalámbrico.

3.2 Hipótesis específicas:

3.2.1 Hipótesis Especifica 1.

Un sistema de seguridad de control de acceso con RADIUS es significativo para determinar el grado de autenticidad en el control del tráfico inalámbrico

3.2.2 Hipótesis Específica 2.

El empleo de un sistema de seguridad del control de acceso con RADIUS mide el grado de autorización del control del tráfico inalámbrico.

3.2.3 Hipótesis Específica 3.

El Desarrollo de un Modelo de Sistema de Administración para la mejora continua en la gestión de usuarios en el control de tráfico inalámbrico mejora su performance.

3.3 Identificación de variables:

3.3.1 Variable Independiente:

Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS

3.3.2 Variable Dependiente:

Grado de autenticación, autorización del control del tráfico inalámbrico

3.4 Operacionalización de variables:

3.4.1 Variable Independiente:

Desarrollo e Implementación de un Sistema de Seguridad de Control de Acceso con RADIUS

3.4.2 Variable Dependiente:

- Grado de grado de autenticación del control del tráfico inalámbrico
- Grado de grado de autorización del control del tráfico inalámbrico

3.5 Matriz de consistencia: Tabla 1.

TITULO	PROBLEMAS	OBJETIVOS	HIPOTESIS	VARIABLE
Desarrollo e Implementación de un sistema de Control de Acceso redes inalámbricas mediante RADIUS en el Instituto Geofísico del Perú - IGP	**Problema General**: ¿Qué efectos produce un sistema de Seguridad de Control de Acceso con RADIUS en el grado de autenticación y autorización en el control de tráfico inalámbrico?	**Objetivo General**: Implementar efectos que produce un sistema de Seguridad de Control de Acceso con RADIUS en el grado de autenticación y autorización del control de tráfico inalámbrico de información.	**Hipótesis General**: El Desarrollo e Implementación de un Sistema de Seguridad de Control de Acceso con RADIUS produce efectos que determina el grado de autenticación y autorización en el control de tráfico inalámbrico.	**Variable Independiente:** Desarrollo e Implementación de un Sistema de Seguridad de Control de Acceso con RADIUS
	Problema Específico 1. ¿Qué resultados produce un sistema de Seguridad de Control de Acceso con RADIUS en el grado de autenticación del control de tráfico inalámbrico de información?	**Objetivo específico 1**.Analizar los efectos que produce un sistema de Seguridad de Control de Acceso con RADIUS en el grado de autenticación en el control de tráfico inalámbrico.	**Hipótesis Especifica 1.** Un sistema de seguridad de control de acceso con RADIUS si es significativo para determinar el grado de autenticidad en el control del tráfico inalámbrico	**Variable Dependiente:** Grado de grado de autenticación del control del tráfico inalámbrico
	Problema específico 2. ¿Cómo repercute un sistema de Seguridad de Control de Acceso con RADIUS en el grado de autorización del control de tráfico inalámbrico de información?	**Objetivo específico 2.** Analizar los efectos que produce un sistema de Seguridad de Control de Acceso con RADIUS en el grado de autorización en el control de tráfico inalámbrico.	**Hipótesis Especifica 2.** El empleo de un sistema de seguridad del control de acceso con RADIUS si es significativo para medir el grado de autorización del control del tráfico inalámbrico.	**Variable Dependiente:** Grado de autorización del control del tráfico inalámbrico
	Problema Específico 3. ¿Cómo repercute el Desarrollo de un Modelo de Administración y gestión de usuarios en el control de tráfico inalámbrico?	**Objetivo específico 3.** Desarrollar un modelo de sistema administrativo y gestión de usuarios en el control de tráfico inalámbrico.	**Hipótesis Especifica 3.**El Desarrollo de un Modelo de Sistema de Administración para la mejora continua en la gestión de usuarios en el control de tráfico inalámbrico mejora su performance.	

Fuente: **Elaboración propia**

CAPITULO IV: RESULTADOS Y DISCUSIÓN

4.1 Tipo y Diseño de Investigación

4.1.1 Tipo de Investigación

Es una investigación de tipo Tecnológica Correlacional. Es tecnológica porque tiene por objetivo Desarrollar e Implementar los efectos que produce un sistema de Seguridad de Control de Acceso con RADIUS. El estudio se realiza en el Instituto Geofísico del Perú – IGP en la Urb. Camacho – Distrito La Molina.

Es una investigación correlacional porque mide el grado de relación entre las variables de estudio el Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS y la otra variable Grado de autenticación y autorización, del control del tráfico inalámbrico.

Debido al problema de Investigación se trata de un estudio no experimental correlacional ya que el estudio tiene como propósito medir el grado de relación que existe entre dos variables, y esto se ajusta a la definición brindada por Hernandez R. Fernandez C. Y Baptista (1981) acerca de los estudios correlacionados.

4.1.2 Diseño de Investigación

Es un diseño transversal no experimental, el cual se muestra en el siguiente diagrama.

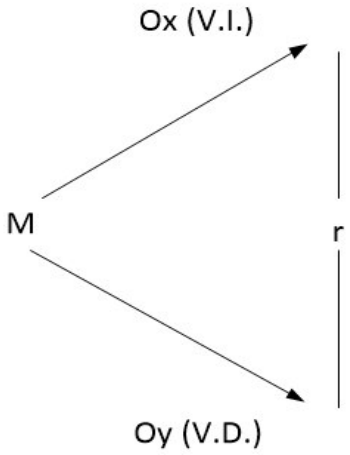


Figura 12: **Diseño de Investigación**.

Fuente: Autor de Tesis

Denotación

M = Muestra de Investigación

Ox = Variable independiente (Sistema de control de acceso con RADIUS)

Oy = Variable Dependiente (Grado de control de Autenticación y Autorización del trafico inalámbrico)

r = Relación entre variable

4.2 Unidad de análisis

El uso de una herramienta que mejore la gestión y distribución de los usuarios en código abierto, mediante el protocolo LDAP con la plataforma phpLDAPadmin, este directorio administra las jerarquías de los usuarios en la institución, de modo que la creación y permisos ya están administrados desde esta plataforma

Servicio de Movilidad Mundial para Universidades e Institutos de Investigación (eduroam) en el IGP. Servicio de movilidad segura desarrollado para la comunidad académica y de investigación, este servicio permite que estudiantes, investigadores y personal de las instituciones participantes tengan conectividad a través de su propio campus y cuando visiten otras instituciones participantes.

4.3 Población de estudio

La población de estudio está conformada por todos los científicos investigadores del Instituto Geofísico del Perú según la información dada por el área de recursos humanos del Instituto Geofísico del Perú un total de 45 Cientificos Investigadores, quienes contribuyen a la población de candidatos al uso del servicio eduroam.

4.4 Tamaño de muestra

Se realizó el estudio con una población de 45 Cientificos Investigadores que realizan labores las sedes de Camacho, Mayorazgo, Jicamarca, Observatorio Vulcanológico y Observatorio de Huancayo

La unidad de Análisis o de Observación fueron 45 usuarios que corresponden a los Científicos de investigadores para lo cual se empleó la siguiente formula

$$\mathrm{n} = \frac{Z^2 p * q^2 * \mathrm{N}}{\mathrm{N}e^2 + Z^2 p * q}$$

Dónde:

n = Tamaño de la muestra
e = 5% = 0.05 (error de estimación)
Z = 1.96 para el 95% de confiabilidad
N = 45 (Universo)
p = 0.50 (probabilidad a favor)
q = 0.50 (Probabilidad en contra)

$$n = \frac{(1.96)^2(0.5)(1-0.5)(45)}{45 * 0.05^2 + 0.5^2(1-0.5)}$$

$$n = \frac{3.8416 * 0.5 * 0.5 * 45}{4.5 * 0.0025 + 0.9604}$$

$$n = \frac{43.218}{1.0604}$$

$$n = 40$$

4.5 Selección de muestra

La muestra es de tipo probabilístico para obtención de la muestra (Cientificos Investigadores) Aleatorio simple. Vale decir que cualquier de los elementos de la población tienen la posibilidad de ser tomados en cuenta

Tabla 2. Cantidad de usuarios encuestados (40 tamaño de muestra)

Item	SEDE	AREA	Cantidad de Personas
1	JICAMARCA	Radio Observatorio de Jicamarca – ROJ	8
2	MAYORAZGO	Sub dirección de Ciencias de la Atmosfera de la Hidrosfera - SDCAH	5
		Sub Dirección de Geofísica y Sociedad – SDGYS	5
3	CAMACHO	Sub dirección de Redes Geofísicas – SDRG	5
		Sub dirección de ciencias de la tierra solida – SDCTS	13
4	HUANCAYO	Observatorio de Huancayo - OHY	2
5	AREQUIPA	Observatorio Vulcanológico del Sur – OVS	2

4.6. Técnicas de recolección de Datos

Encuesta por cuestionarios virtuales, esta encuesta tuvo su fundamento en el enfoque de la percepción de los usuarios, de modo que se mostraba las bondades de un sistema RADIUS y a su vez cual era la percepción en que parámetros debieran ser tomados en cuenta para su respectiva autenticación y autorización en los niveles de control de acceso a la red de la Institución, siendo así unas diez preguntas enfocadas en el sistema de control de acceso con RADIUS , cinco preguntas enfocadas en el grado de Autenticación y otras cinco preguntas enfocadas en el grado de Autorización para el acceso.

A continuación se muestra la encuesta virtual elaborada por el área de Gestión de Proyectos en tecnologías de la Información:

- Variable Independiente: Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS

Tratamiento estadístico

Respuesta 3:

Los resultados obtenidos se presentan siguiendo el orden de los objetivos específicos de la investigación

Objetivo específico N1;

* Analizar los efectos que produce un SSCAR Grado de Aunte en el CTRwi

Objetivo específico N2

* Analizar los efectos que produce un SSCAR Grado de Auto en el CTRWi

Objetivo específico N3

* Desarrollar un modelo de SAGU CtrlWi

Tratamiento estadístico: Para desarrollar los objetivos de la investigación se aplicaron los siguientes procedimientos estadísticos

* Estadística Descriptiva: Nos ha permitido describir los datos, valores obtenidos por cada variable.

Descripción de frecuencias, media aritmética, desviación estándar

* Estadística Inferencial: Para generalizar los resultados de la muestra a la población, se utilizó distribución muestral, chi cuadrado de Pearson, correlación de Spearman

1. Grado de Autenticación en el control del tráfico inalámbrico
   1.1 El grado de autenticación del control trafico inalámbrico
   La confiabilidad fue precisado utilizando el método Alfa de Cronbach, los resultados mostraron un Alpha de 0.94 en la prueba demostrando ser un buen instrumento para evaluar el grado de autenticación
   1.2

Tabla 3.

Pregunta 1 Encuesta Virtual

1. ¿Considera que la Institución debe registrar a cualquier usuario con un sistema o servidor de control?		
Opción	Número de usuarios	Porcentaje
Totalmente	2	5%
En gran Medida	6	15%
En alguna Medida	13	33%
En poca Medida	10	25%
De ningun modo	9	23%

Fuente: ***Datos tomados de - Encuesta Virtual IGP***

De los encuestados un 5% indico estar totalmente de acuerdo con su sistema de control para el registro de cualquier usuario en la institución, un 15% indico que en gran medida, un 33% indico que en alguna medida y resto entre en poca medida y de ningún modo.

Se observa que la gran mayoría acepta que es necesario el control de cada usuario mediante alguna herramienta electrónica para mantener un registro no solo de ingreso a la entidad, si no de actividad que realizara internamente.

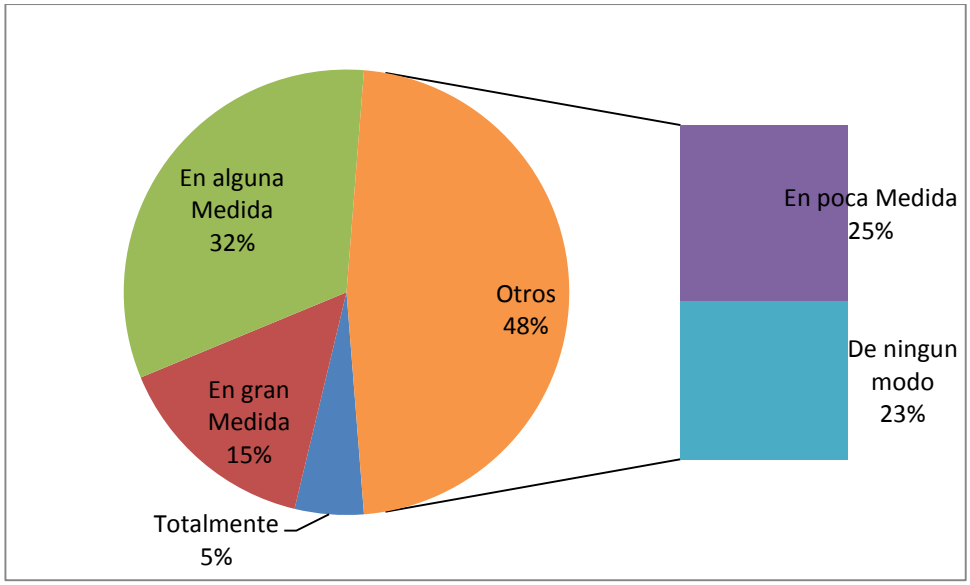


Figura 13: **Estadísticas arrojadas con respecto a los empleados sobre la pregunta** *1*

Fuente: encuesta virtual IGP

Tabla 4

Pregunta 2 Encuesta Virtual

2. ¿Consideras que un usuario de la Institución debiera tener acceso a todas las redes locales del IGP		
Opción	Número de usuarios	Porcentaje
Totalmente	1	3%
En gran Medida	8	20%
En alguna Medida	17	43%
En poca Medida	12	30%
De ningún modo	2	5%

Fuente. Datos tomados de - Encuesta Virtual IGP

De los resultados se infiere que un 3% está totalmente de acuerdo en que los usuarios de la Institución tengan acceso a todas las redes locales inalámbricas, un 20 % indico en gran medida, un 43% en alguna medida, un 30% en poca medida y un 5% de ningún modo.

Es baja la consideración que los usuarios de la Institución accedan a todas las redes Inalámbricas, pero en promedio indicaron que el acceso es necesario en alguna medida, lo cual en base a ello las políticas continuaran con restricciones para acceder a ciertas zonas de cobertura inalámbrica.

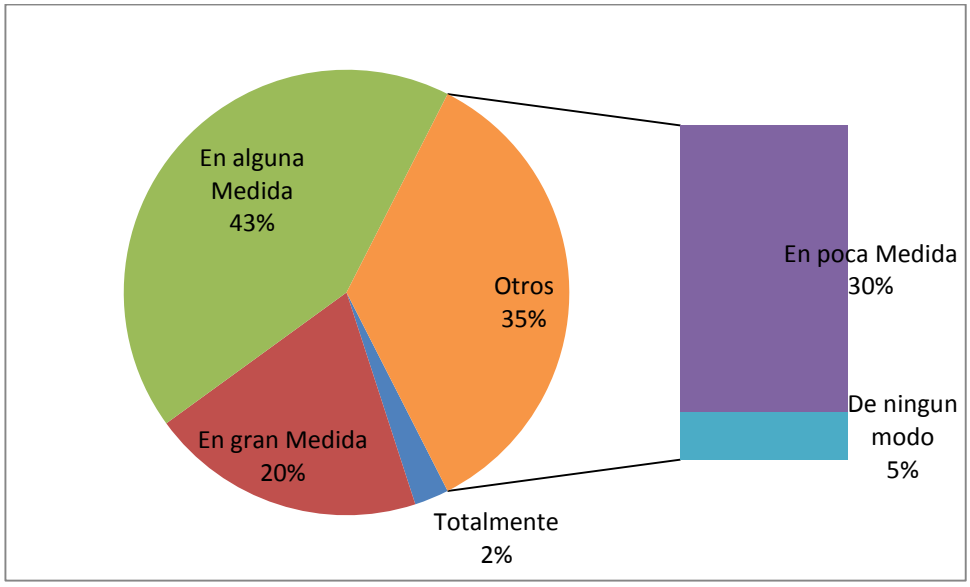


Figura 14: **Estadísticas arrojadas con respecto a los empleados sobre la pregunta** *2.*

Fuente. IGP - encuesta virtual**.**

Tabla 5.

Pregunta 3 Encuesta Virtual

3. ¿Consideras que los puntos inalámbricos brindan un estándar óptimo de seguridad de información?		
Opción	Número de usuarios	Porcentaje
Totalmente	1	3%
En gran Medida	3	8%
En alguna Medida	15	38%
En poca Medida	12	30%
De ningún modo	9	23%

Fuente: Datos tomados de - Encuesta Virtual IGP

De los resultados se infiere que un 3 % considera totalmente que los puntos inalámbricos brindan un estándar óptimo de seguridad totalmente, un 8% índico que en gran medida, un 38% que en alguna medida, un 30 % en alguna medida y solo 23 % de ningún modo.

La percepción de los empleados sobre los estándar de seguridad en la red inalámbrica se considera aceptable, pero esto aceptación se lograra consolidar un la implementación del servidor RADIUS usando el servicio eduroam.

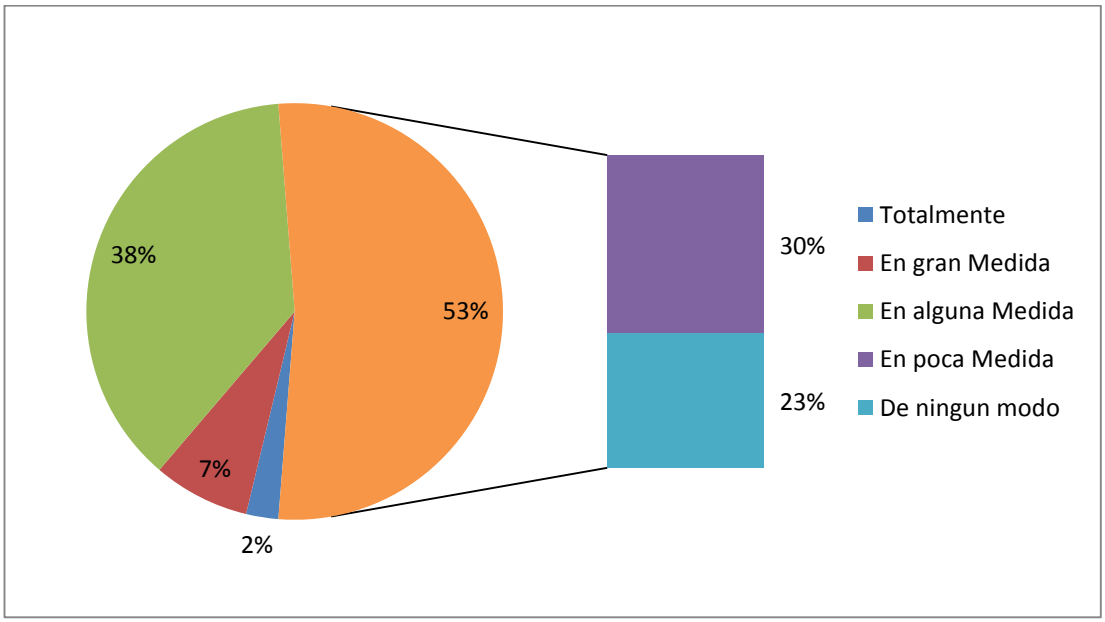


Figura 15: **Estadísticas arrojadas pregunta 3**

Fuente: IGP – Encuesta virtual.

Tabla 6.

Pregunta 4 Encuesta Virtual

4. ¿Tienes conocimiento de algún sistema de control de acceso a la red?		
Opción	Número de usuarios	Porcentaje
Totalmente	0	0%
En gran Medida	3	8%
En alguna Medida	16	40%
En poca Medida	15	38%
De ningún modo	6	15%

Fuente. Datos tomados de - Encuesta Virtual IGP

Estos resultados confirman que los empleados encuestados tienen en su mayoría conocimiento de la un servicio de control de acceso en la Institución, lo cual nos permitirá introducir con mayor disponibilidad de una nueva plataforma de control de acceso con mayores bondades en la seguridad informática.

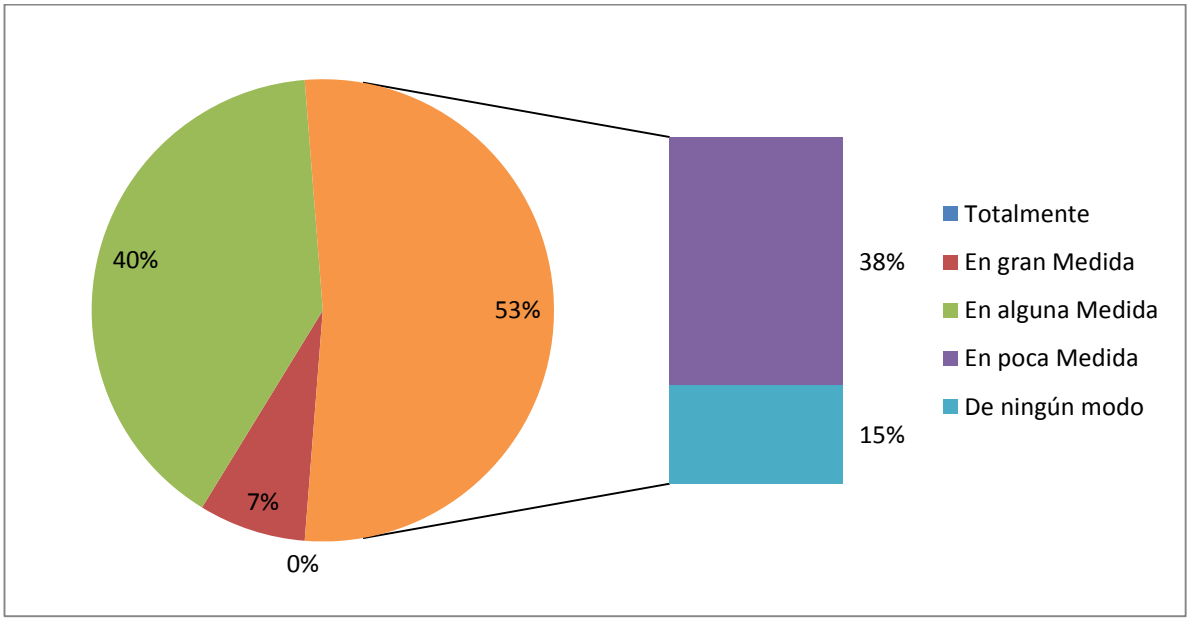


Figura 16: ***Estadísticas arrojadas pregunta 4 Ref.: IGP- Encuesta virtual***

Fuente. IGP – *Encuesta virtual*

Tabla 7.

Pregunta 5 Encuesta Virtual

5. Luego de haber recibido información por parte de la oficina de Tecnologías OTIDG ¿Cree que un servicio RADIUS sería lo más óptimo para la Institución?		
Opción	Número de usuarios	Porcentaje
Totalmente	1	3%
En gran Medida	5	13%
En alguna Medida	10	25%
En poca Medida	12	30%
De ningún modo	12	30%

Fuente. **Datos tomados de - Encuesta Virtual IGP**

Se observa que la mayoría ha quedado satisfecha y es una gran oportunidad de mejorar la implementación de seguridad informática con un servicio RADIUS mejorado el cual brinda servicios de valor agregado a la Institución.

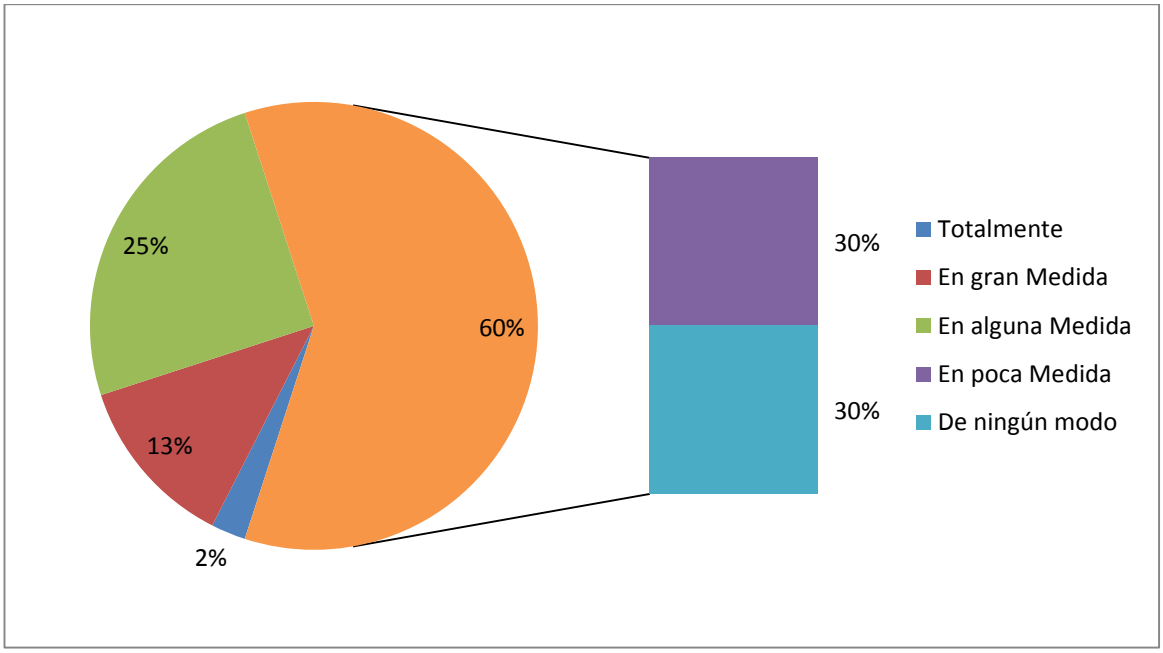


Figura 17: **Estadísticas arrojadas pregunta 5. Ref. IGP- Encuesta virtual.**

Fuente. IGP – Encuesta virtual

Tabla 8.

Pregunta 6 Encuesta Virtual

6. Consideras que debe existir un servicio que identifique la pertenencia a la Institución para acceder a la red Local del IGP		
Opción	Número de usuarios	Porcentaje
Totalmente	7	18%
En gran Medida	15	38%
En alguna Medida	13	33%
En poca Medida	4	10%
De ningún modo	1	3%

Fuente. Datos tomados de - Encuesta Virtual IGP

Observamos que un gran sector de los encuestados requiere y hace mención a la necesidad de acceder como usuario perteneciente a la Institución por algún servicio de red interno. Esto conlleva a usar métodos de restricción solo para personal interno del IGP.

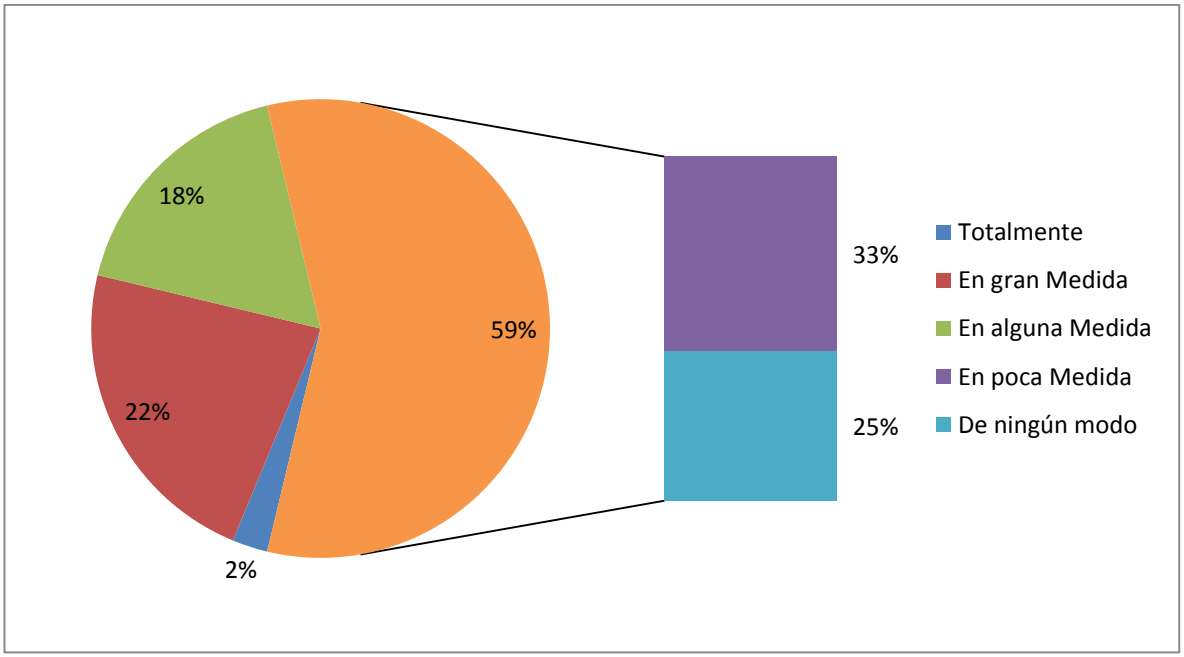


Figura 18: **Estadísticas pregunta 6. Fuente: IGP-Encuesta virtual.**

Fuente. IGP – Encuesta virtual

Tabla 9.

Pregunta 7 Encuesta Virtual

7. ¿Consideras que el uso de un certificado digital al acceder a la red local te garantiza mayor seguridad en la red del IGP?		
Opción	Número de usuarios	Porcentaje
Totalmente	2	5%
En gran Medida	6	15%
En alguna Medida	10	25%
En poca Medida	13	33%
De ningún modo	9	23%

Fuente. Datos tomados de - Encuesta Virtual IGP

El análisis de los resultados nos revela la que los perciben que la implementación de un certificado digital brindara mayor seguridad al acceder a los servicios de red local, esto manifiesta la importancia de la confidencialidad de los datos mediante técnicas de seguridad para un mejor control en resguardo de la información.

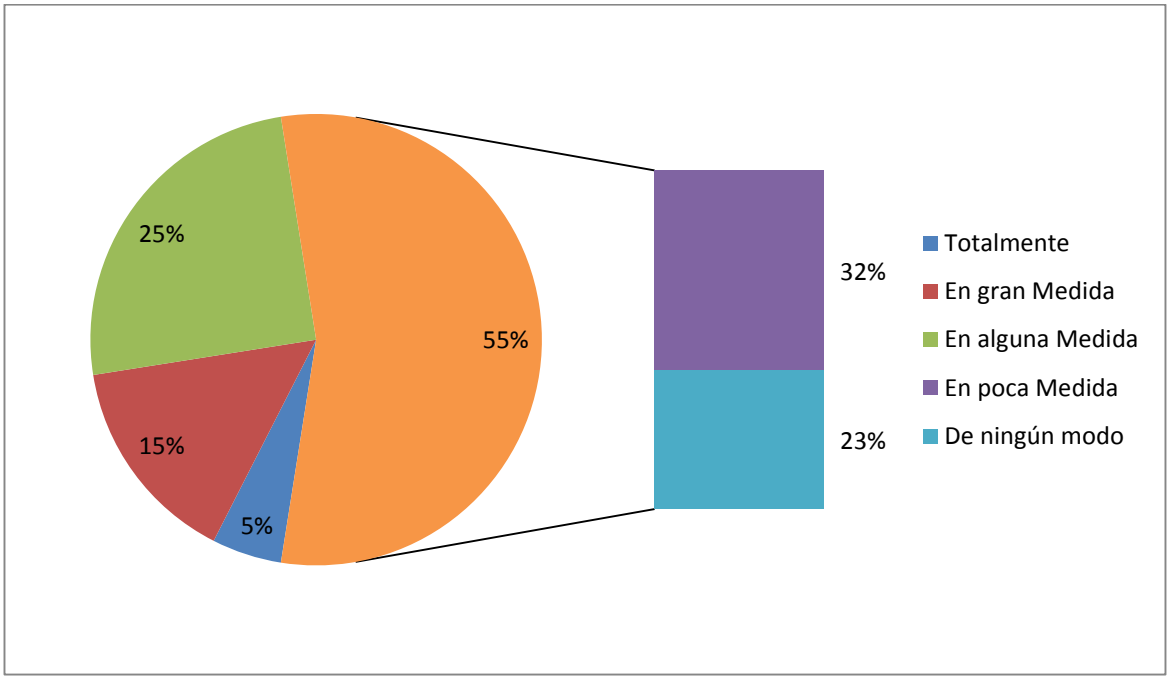


Figura 19: **Estadísticas arrojadas pregunta 7**.

Fuente. IGP-Encuesta virtual

Tabla 10.

Pregunta 8 Encuesta Virtual

8. ¿Consideras que el actual sistema inalámbrico es seguro en la red Local?		
Opción	Número de usuarios	Porcentaje
Totalmente	1	3%
En gran Medida	8	20%
En alguna Medida	12	30%
En poca Medida	17	43%
De ningún modo	2	5%

Fuente: Datos tomados de - Encuesta Virtual IGP

El análisis al observar estos resultados nos indican que existe confianza en la privacidad del acceso a la información cuando se solicita el servicio inalámbrico, lo que conlleva a continuar manteniendo esta confianza en los usuarios con nuevas propuestas tecnológicas.

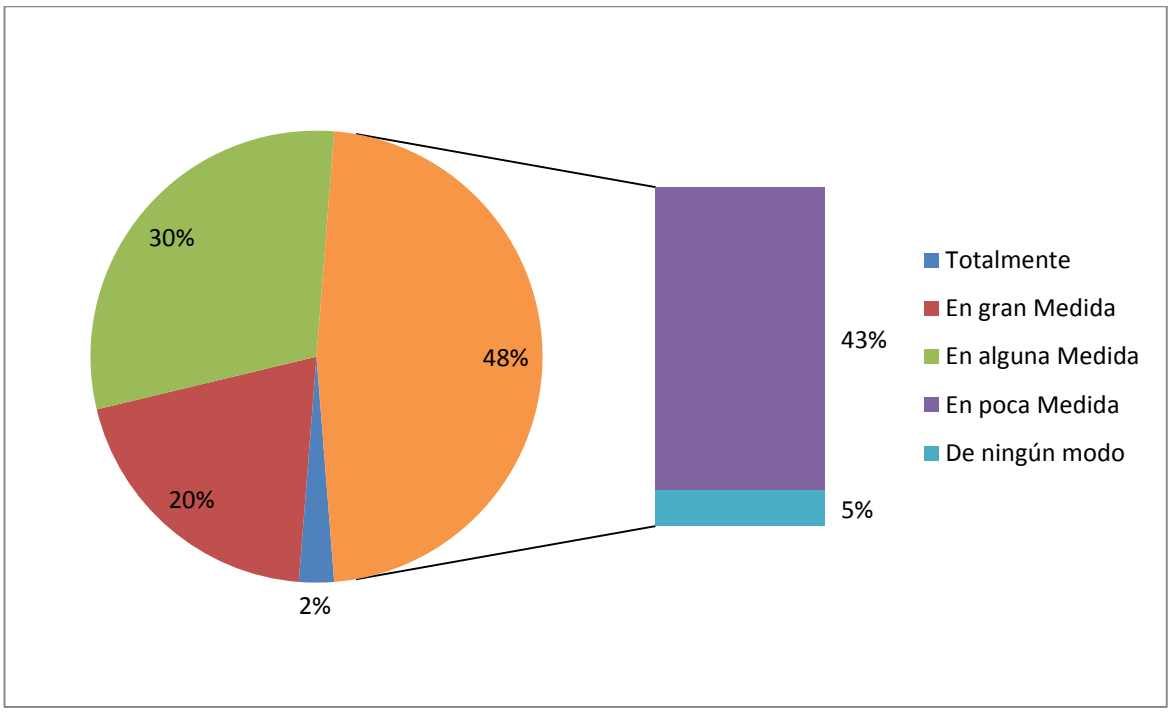


Figura 20: **Estadísticas arrojadas pregunta 8.**

Fuente. IGP - Encuesta virtual

Tabla 11.

Pregunta 9 Encuesta Virtual

9. ¿Consideras que la contraseña de acceso a los puntos inalámbricos debe ser la misma para todos los usuarios?		
Opción	Número de usuarios	Porcentaje
Totalmente	1	3%
En gran Medida	3	8%
En alguna Medida	12	30%
En poca Medida	15	38%
De ningún modo	9	23%

Fuente: Datos tomados de - Encuesta Virtual IGP

Estos resultados nos dan un claro comportamiento del usuario, su preferencia por usar una misma contraseña para acceder al servicio inalámbrico, sin embargo esto contrae riesgos que esta contraseña se divulgue a personas ajenas a la institución, lo cual conllevar a pérdida o infiltraciones a la red local.

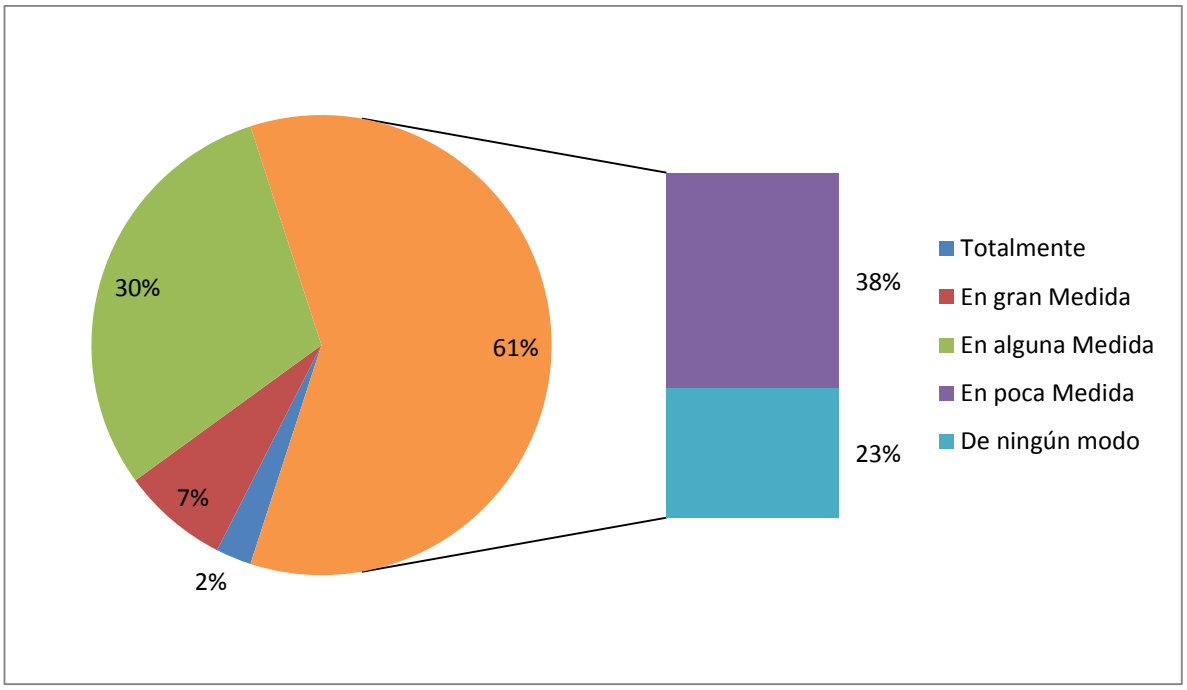


Figura 21: **Estadísticas arrojadas pregunta 9**

Fuente. IGP- Encuesta virtual

Tabla 12.

Pregunta 10 Encuesta Virtual

10. ¿Consideras que luego de hacer uso del servicio eduroam fuera de las instalaciones de la institución este servicio debe implementarse en todas las sedes del IGP		
Opción	Número de usuarios	Porcentaje
Totalmente	0	0%
En gran Medida	3	8%
En alguna Medida	17	43%
En poca Medida	13	33%
De ningún modo	7	18%

Fuente. Datos tomados de - Encuesta Virtual IGP

El análisis sobre estos resultados confirma que existe que más del 80 % de los encuestados se encuentra convencido de la implementación del servicio eduroam viendo que ya tuvo experiencia con las bondades a las que puede conectase en diversas Instituciones a nivel nacional e Internacional.

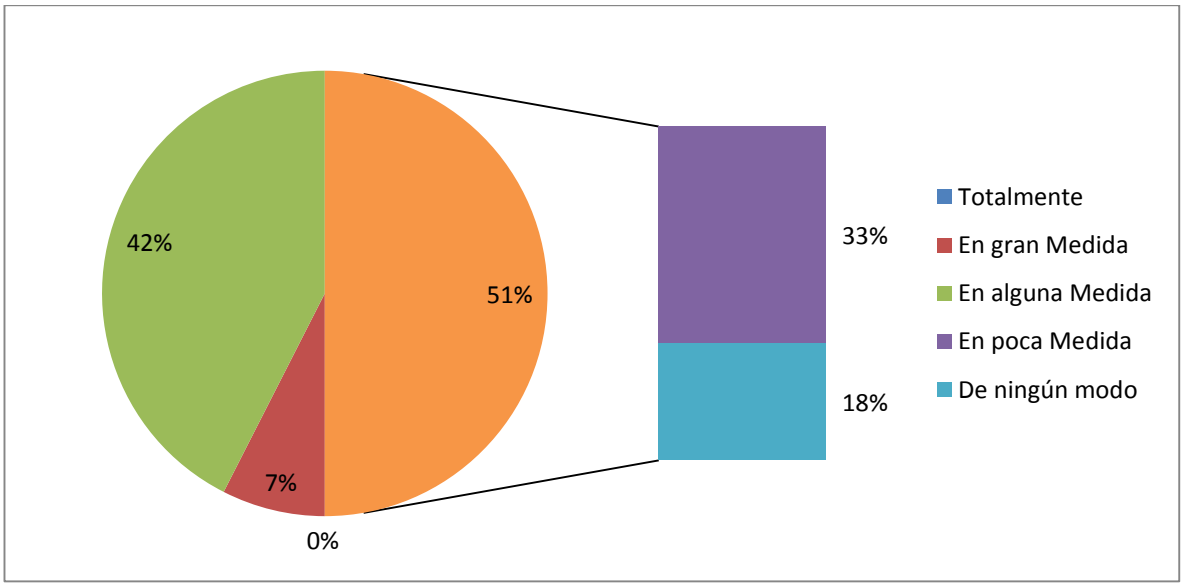


Figura 22: **Estadísticas arrojadas pregunta 10**

Fuente. IGP- Encuesta virtual

- Variable Dependiente 1: Grado de grado de autenticación del control del tráfico inalámbrico

Tabla 13.

Pregunta 11 Encuesta Virtual

11. ¿Consideras como parte de brindar mayor seguridad en la red inalámbrica, que el sistema te solicita algún certificado de seguridad?		
Opción	Número de usuarios	Porcentaje
Totalmente	1	3%
En gran Medida	9	23%
En alguna Medida	7	18%
En poca Medida	13	33%
De ningún modo	10	25%

*Fuent.:*Datos tomados de - Encuesta Virtual IGP

Cabe resaltar que al hacer uso de un certificado digital este certificado queda en el equipo del usuario una vez y para que en otra oportunidad reconozca que el equipo pertenece a la Institución o en algún momento accedió y no vuelva a solicitarlo.

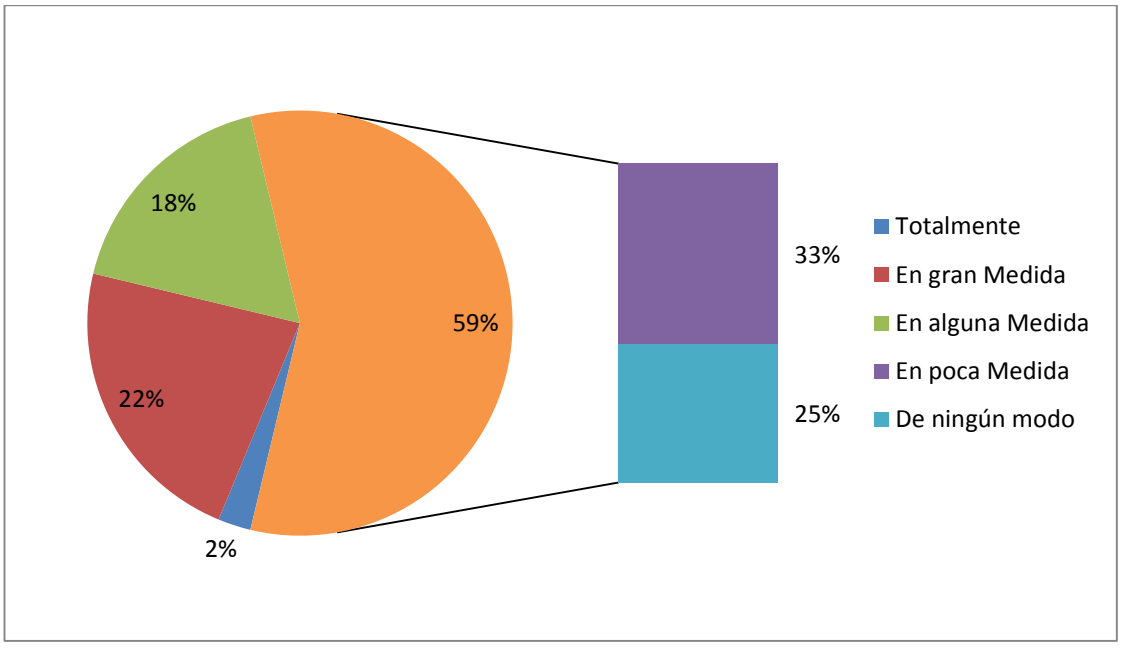


Figura 23: **Estadísticas pregunta 11**

Fuente: IGP - Encuesta virtual

Tabla 14.

Pregunta 12 Encuesta Virtual

12. ¿Consideras que es necesario la implementación de algún sistema de seguridad donde te pida autenticarte con tu usuario y contraseña de correo electrónico como modo de autenticarte este año?		
Opción	Número de usuarios	Porcentaje
Totalmente	2	5%
En gran Medida	6	15%
En alguna Medida	10	25%
En poca Medida	13	33%
De ningún modo	9	23%

Fuente. Datos tomados de - Encuesta Virtual IGP

Se analiza el comportamiento del usuario encuestado quien ha respondido conveniente el uso del usuario y contraseña del correo electrónico como modo de autenticarse es lo más funcional para el acceso a servicios locales, debido a que en muchos casos los usuarios y contraseñas suelen ser diversos.

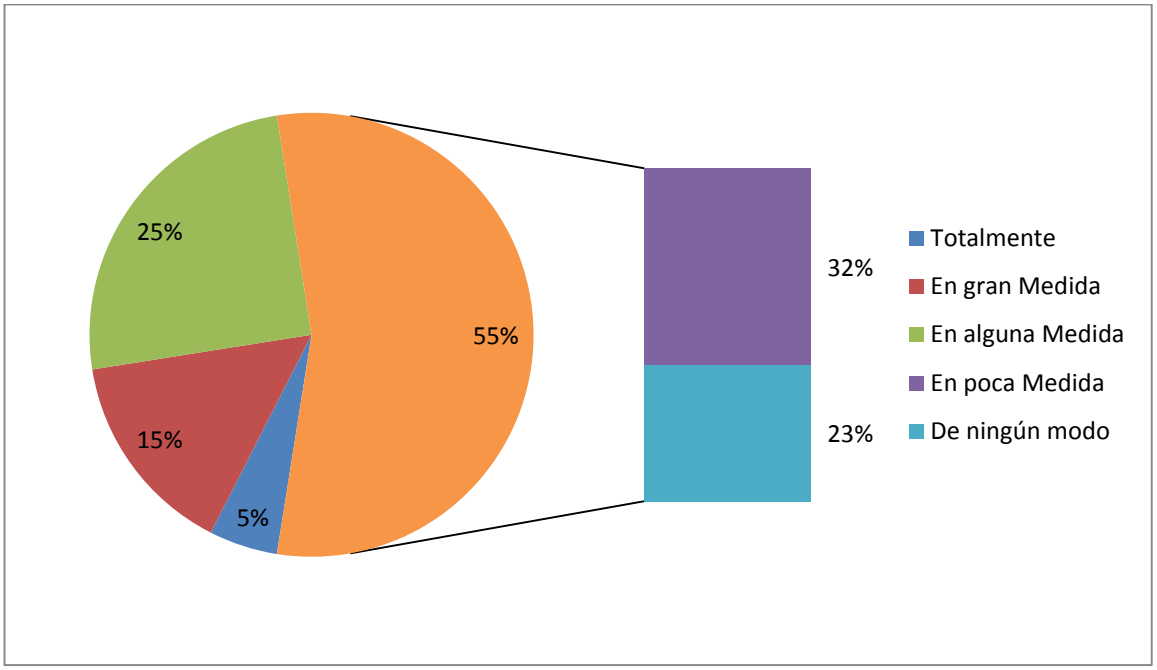


Figura 24: ***Estadísticas arrojadas pregunta 12***

Fuente. IGP - Encuesta virtual

Tabla 15.

Pregunta 13 Encuesta Virtual

13. ¿Consideras que el grado de Autenticación para el acceso a los servicios de Red del IGP debe estar dado por la dirección IP del usuario?		
Opción	Número de usuarios	Porcentaje
Totalmente	1	3%
En gran Medida	8	20%
En alguna Medida	12	30%
En poca Medida	17	43%
De ningún modo	2	5%

Fuente. Datos tomados de - Encuesta Virtual IGP

Los resultados mostraron que la mayoría de los encuestados tiene conocimiento de su dirección IP por lo que asume que depende de esta dirección sus privilegios.

Esto nos conlleva a plantearnos que un usuario con mayor conocimiento técnico podría llegar a suplantar su dirección Ip, por lo tanto al área de Tecnologías nos pone un reto para mejorar el sistema de acceso de Autenticación a los servicios de Red local.

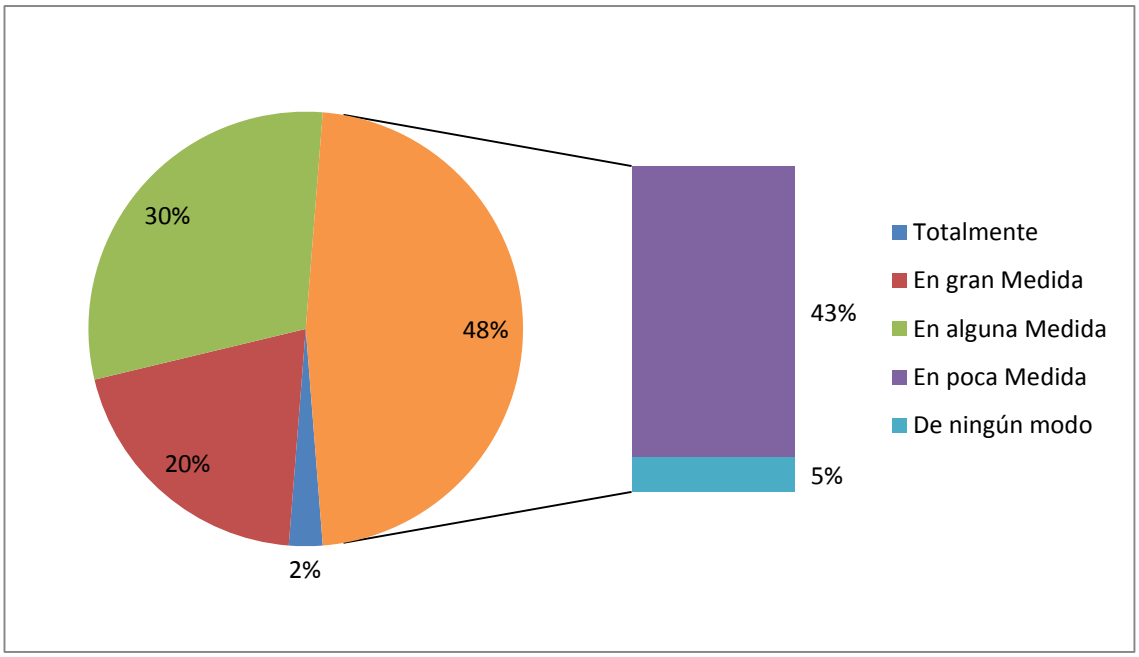


Figura 25: Estadísticas arrojadas pregunta 13. Fuente: IGP - Encuesta virtual

Fuente. IGP – Encuesta virtual

Tabla 16.

Pregunta 14 Encuesta Virtual

14. Consideras que al acceder a los servicios de red de la institución ¿Deberías usar tu cuenta y usuario de correo electrónico para autenticarte?		
Opción	Número de usuarios	Porcentaje
Totalmente	1	3%
En gran Medida	3	8%
En alguna Medida	12	30%
En poca Medida	15	38%
De ningún modo	9	23%

Los resultado nos muestran que el usuario percibe como como una práctica que ayuda al usuario considerandos como funcional que su acceso a los servicio deba darse con su mismo nombre de cuenta de correo electrónico, cabe resaltar que algunos accesos a los servicios de red sea acceso a impresiones o acceso a fotocopia de la Institución no cumplen con este patrón o estándar el cual debe normalizarse.

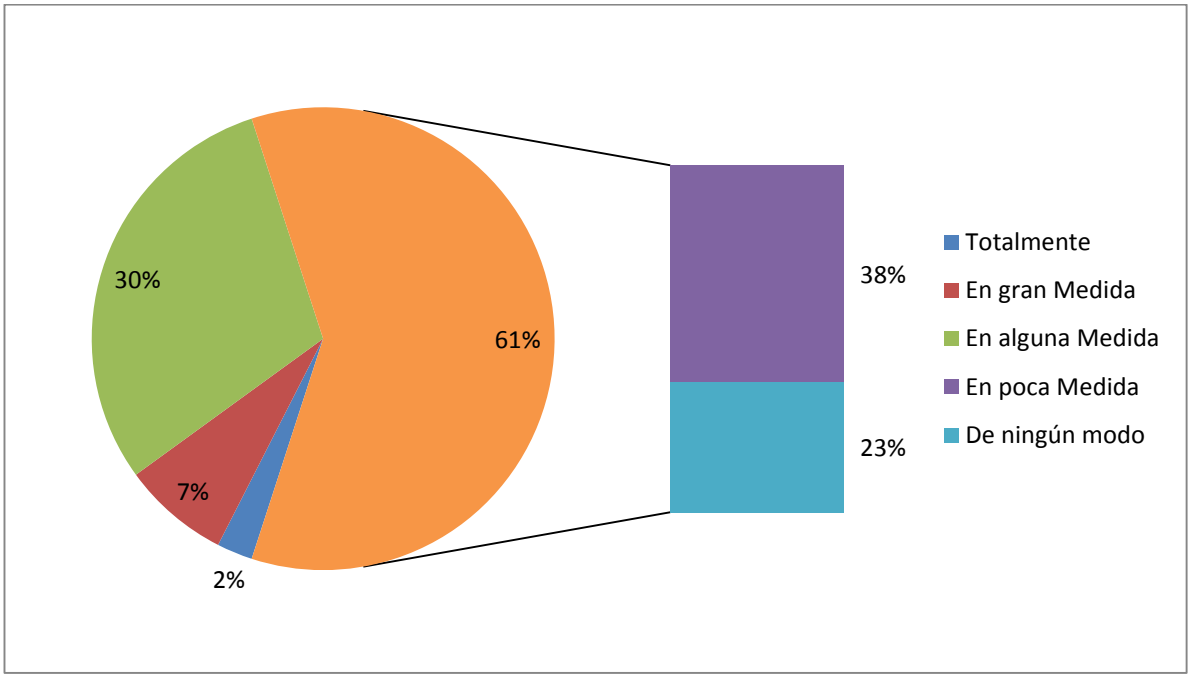


Figura 26: **Estadísticas arrojadas pregunta 14**.

Fuente. IGP - Encuesta virtual

Tabla 17.

Pregunta 15 Encuesta Virtual

15. Consideras que para la Autenticación de los usuarios del IGP a los servicios de Red solo deberían usar su usuario y contraseña en todos los accesos locales de red.		
Opción	Número de usuarios	Porcentaje
Totalmente	0	0%
En gran Medida	3	8%
En alguna Medida	17	43%
En poca Medida	13	33%
De ningún modo	7	18%

Fuente. Datos tomados de - Encuesta Virtual IGP

De los resultados mostrados nos muestra que más del 50 % considera el uso temporal de una VPN cuando no se encuentre dentro de las instalaciones de la institución, este servicio cumple estándares de seguridad comparado a un acceso web que podría también darse sin embargo el acceso a web tiene mayores vulnerabilidades y por ende podría existir un ataque a los servicios de red local.

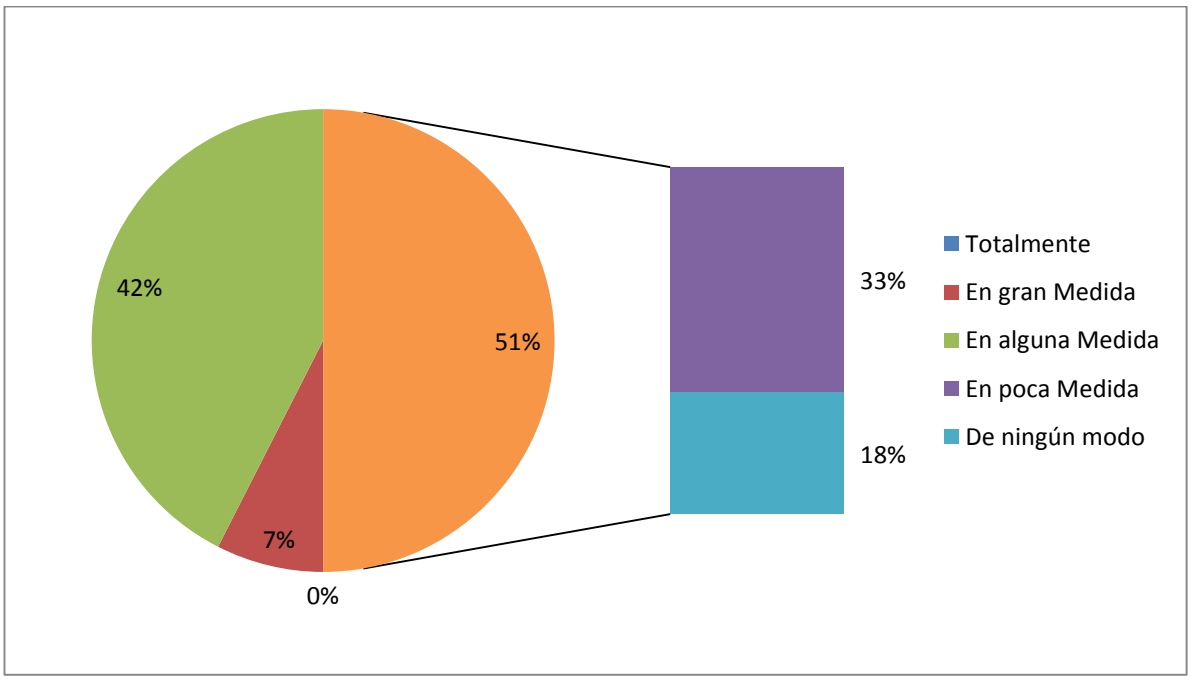


Figura 27: **Estadísticas arrojadas pregunta 15.**

Fuente. IGP - Encuesta virtual

Tabla 18.

Pregunta 16 Encuesta Virtual

16. Consideras que los usuarios invitados que se conecten al servicio inalámbrico deben tener acceso libre a Internet sin usar la red local		
Opción	Número de usuarios	Porcentaje
Totalmente	1	3%
En gran Medida	3	8%
En alguna Medida	12	30%
En poca Medida	15	38%
De ningún modo	9	23%

Fuente. Datos tomados de - Encuesta Virtual IGP

Los resultados nos dan como referente que si un usuario invitado accede a internet en la Institución no debería hacer uso de los recursos locales, plantear esta solución conlleva a separar un servicio de Internet que sea divergente de la red local a fin de no involucrar algún riesgo con equipos que pudieran estar infectados o ser proclives en emitir vulneración de la red Local.

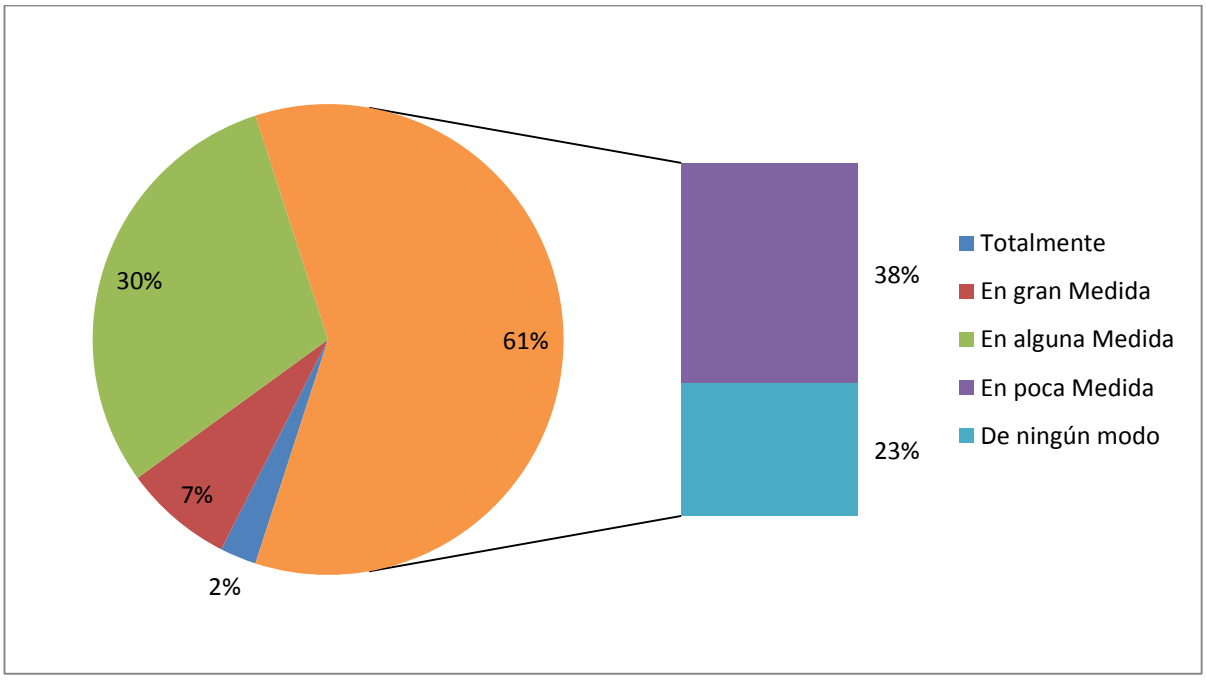


Figura 28: **Estadísticas arrojadas pregunta 16.**

Fuente: IGP- Encuesta virtual

Tabla 19.

Pregunta 17 Encuesta Virtual

17. Consideras que la autorización a accesos internos en la institución se debe a tus funciones laborales.		
Opción	Número de usuarios	Porcentaje
Totalmente	1	3%
En gran Medida	8	20%
En alguna Medida	12	30%
En poca Medida	17	43%
De ningún modo	2	5%

Fuente. Datos tomados de - Encuesta Virtual IGP

De los resultados observamos que solo un 13 % indico estar totalmente de acuerdo sin embargo el grueso de las respuestas se encuentra con más del 70 % en afirma que sea el acceso según tus funciones laborales a la red local.

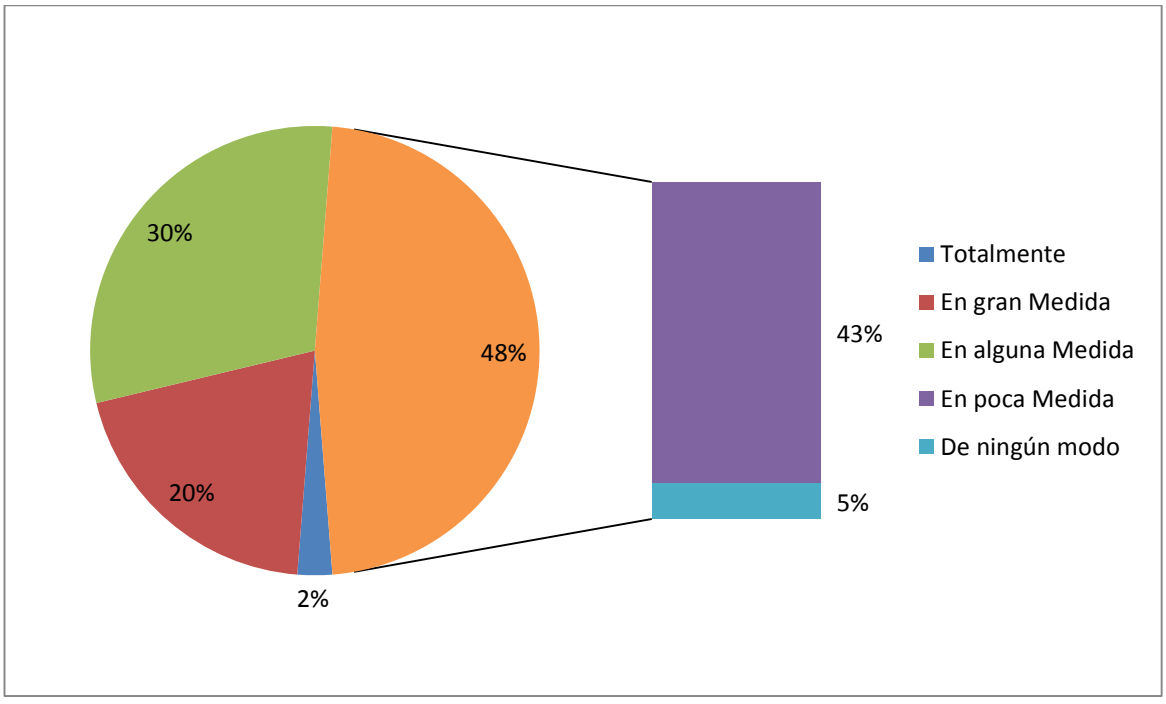


Figura 29: **Estadísticas arrojadas pregunta 17**

Fuente. IGP-Encuesta virtual

Tabla 20.

Pregunta 18 Encuesta Virtual

18. ¿Consideras que un usuario invitado que utilice el servicio eduroam tenga la autorización al acceder a la red local a redes sociales?		
Opción	Número de usuarios	Porcentaje
Totalmente	1	3%
En gran Medida	5	13%
En alguna Medida	12	30%
En poca Medida	10	25%
De ningún modo	12	30%

Fuente. Datos tomados de - Encuesta Virtual IGP

Al analizar el servicio eduroam el cual es un servicio para investigadores y de movilidad mundial, las instituciones que usa este servicio son vistas como Instituciones de confianza por lo cual sus usuarios acceden a información de Investigación neta como publicaciones o artículos científicos, por lo que el acceso a este tipo de información no implica mayor riesgo siempre y cuando se salvaguarde la integridad de estos documentos.

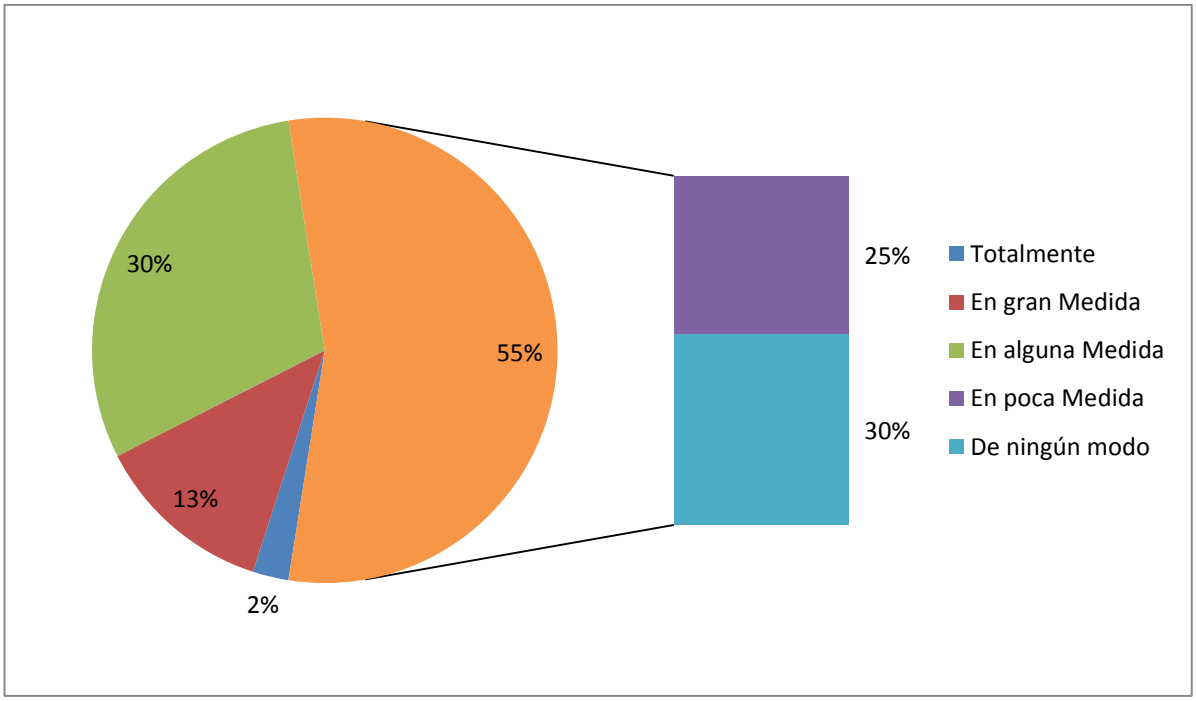


Figura 30: **Estadísticas arrojadas pregunta 18**

Fuente. IGP-Encuesta virtual

Tabla 21.

Pregunta 19 Encuesta Virtual

19. ¿Consideras que las autorizaciones de acceso a la red deberían darse por el nombre de usuario y Área a la que pertenece el empleado?		
Opción	Número de usuarios	Porcentaje
Totalmente	0	0%
En gran Medida	3	8%
En alguna Medida	15	38%
En poca Medida	16	40%
De ningún modo	6	15%

Fuente. Datos tomados de - Encuesta Virtual IGP

Estos resultados muestran la percepción de los empleados encuestados, que según el área al que pertenece debe ser su acceso, sin embargo dentro de cada área también existen funciones que requieren distintos accesos por lo que debe evaluarse de manera específica puesto que las labores de un empleado no necesariamente están sujetas al área al que pertenece.

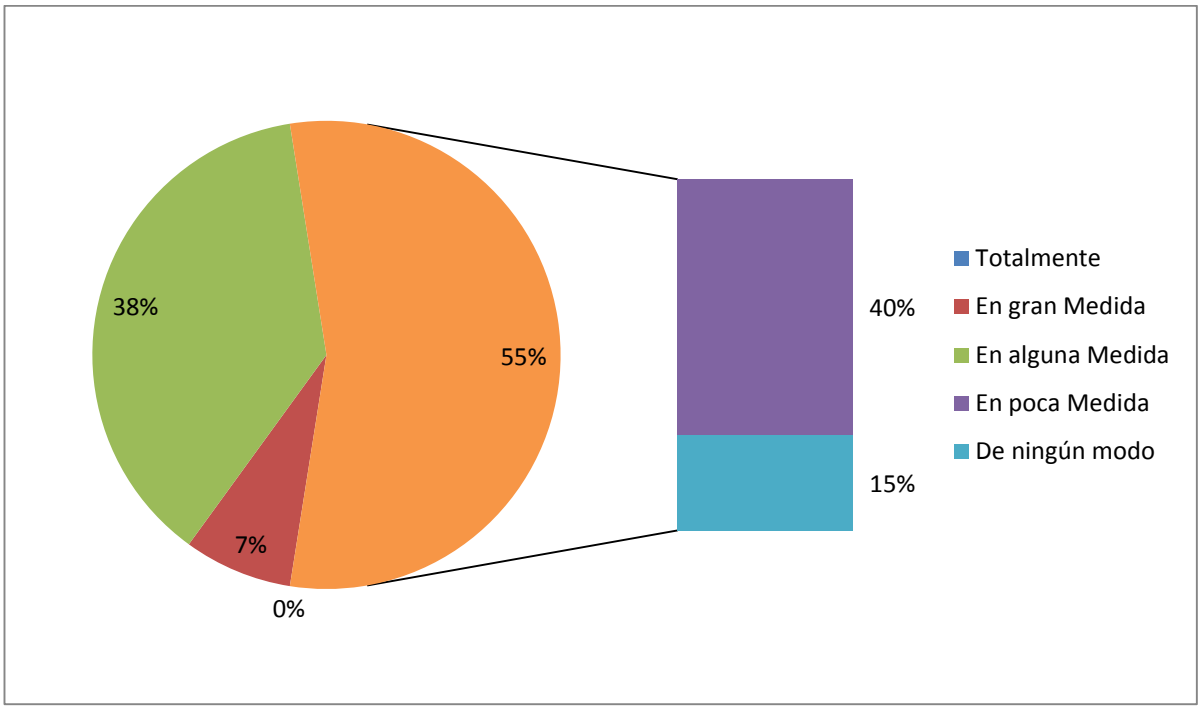


Figura 31: **Estadísticas arrojadas pregunta 19.**

Fuente. IGP-Encuesta virtual

Tabla 22.

Pregunta 20 Encuesta Virtual

20. Consideras que para el acceso inalámbrico solo deberías usar tu cuenta y contraseña de correo electrónico.		
Opción	Número de usuarios	Porcentaje
Totalmente	2	5%
En gran Medida	6	15%
En alguna Medida	10	25%
En poca Medida	13	33%
De ningún modo	9	23%

Fuente. Datos tomados de - Encuesta Virtual IGP

Más del 70 % indico estar de acuerdo que las autorizaciones con accesos sin restricción deban ser por un periodo determinado de modo que el usuario deberá tener en cuenta el uso del servicio de Internet.

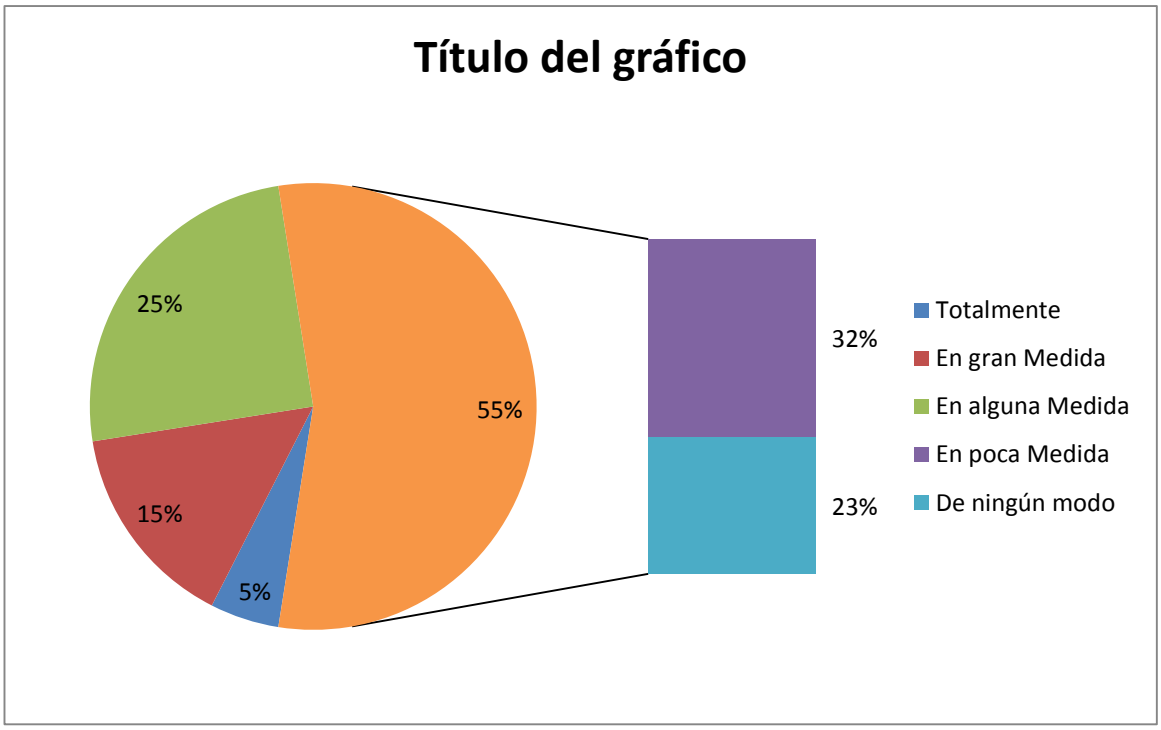


Figura 32: **Estadísticas arrojadas pregunta 20.**

Fuente. IGP- Encuesta virtual

4.7. Prueba de Hipótesis

Tabla 23: **Prueba del CHI-CUADRADO**

Desarrollo de un SSACR					Grado de Autenticidad					Grado de Autorizacion					Modelo de Administración				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
3	3	5	3	4	5	3	3	5	5	5	3	3	5	5	5	3	4	3	3
4	3	4	4	3	3	4	3	4	4	3	4	3	4	4	4	3	3	4	4
5	3	3	4	5	4	5	3	3	4	4	5	3	3	4	3	3	5	4	5
3	2	1	2	3	2	3	2	1	3	2	3	2	1	3	1	2	3	2	3
3	2	5	2	3	2	3	2	5	3	2	3	2	5	3	5	2	3	2	3
5	5	5	4	3	4	5	5	5	3	4	5	5	5	3	5	5	3	4	5
2	2	2	3	1	2	2	2	2	2	2	2	2	2	2	2	2	1	3	2
5	4	5	5	4	5	5	4	5	4	5	5	4	5	4	5	4	4	5	5
1	2	3	3	2	2	1	2	3	3	2	1	2	3	3	3	2	2	3	1
5	4	4	4	5	5	5	4	4	4	5	5	4	4	4	4	4	5	4	5
1	2	2	3	2	2	1	2	2	2	2	1	2	2	2	2	2	2	3	1
2	3	3	3	2	1	2	3	3	3	1	2	3	3	3	3	3	2	3	2
5	4	4	5	3	4	5	4	4	5	4	5	4	4	5	4	4	3	5	5
4	4	4	4	4	3	4	4	4	4	3	4	4	4	4	4	4	4	4	4
3	3	5	5	5	5	3	3	5	5	5	3	3	5	5	5	3	5	5	3
3	2	2	3	3	2	3	2	2	3	2	3	2	2	3	2	2	3	3	3
2	3	4	4	4	2	2	3	4	4	2	2	3	4	4	4	3	4	4	2
5	4	4	4	5	3	5	4	4	4	3	5	4	4	4	4	4	5	4	5
5	5	3	3	5	5	5	5	3	5	5	5	5	3	5	3	5	5	3	5
3	3	3	3	4	4	3	3	3	3	4	3	3	3	3	3	3	4	3	3
4	4	4	4	4	4	4	4	4	3	4	4	4	4	3	4	4	4	4	4
4	3	5	5	5	5	4	3	5	4	5	4	3	5	4	5	3	5	5	4
4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	4	5	4	4
4	4	4	3	3	3	4	4	4	3	3	4	4	4	3	4	4	3	3	4
5	3	3	3	5	4	5	3	3	3	4	5	3	3	3	3	3	5	3	5
2	1	3	3	2	2	2	1	3	2	2	2	1	3	2	3	1	2	3	2
2	2	3	3	3	3	2	2	3	3	3	2	2	3	3	3	2	3	3	2
3	4	4	4	4	4	3	4	4	3	4	3	4	4	3	4	4	4	4	3
4	4	5	5	5	4	4	4	5	5	4	4	4	5	5	5	4	5	5	4
3	4	4	3	3	4	3	4	4	3	4	3	4	4	3	4	4	3	3	3
4	4	3	4	4	5	4	4	3	3	5	4	4	3	3	3	4	4	4	4
5	4	5	3	3	5	5	4	5	4	5	5	4	5	4	5	4	3	3	5
4	4	5	5	5	5	4	4	5	4	5	4	4	5	4	5	4	5	5	4
4	4	4	4	4	5	4	4	4	4	5	4	4	4	4	4	4	4	4	4
2	2	3	4	3	2	2	2	3	3	2	2	2	3	3	3	2	3	4	2
3	3	4	3	5	4	3	3	4	5	4	3	3	4	5	4	3	5	3	3
3	3	3	2	2	3	3	3	3	3	3	3	3	3	3	3	3	2	2	3
4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	3	3	4	3	3	4	3	3	3	3	4	3	3	3	3	3	3	4	4

Fuente. Resultados de la encuesta virtual para el análisis del Chi Cuadrado

4.7.1 Contrastación de la Primera Hipótesis Específica.

4.7.1.1 Estableciendo Hipótesis

- H_0: Un sistema de seguridad de control de acceso con RADIUS No es significativo para determinar el grado de autenticidad en el control del tráfico inalámbrico
- H_1: Un sistema de seguridad de control de acceso con RADIUS es significativo para determinar el grado de autenticidad en el control del tráfico inalámbrico

Si el ***p*** valor asociado al estadístico de contrastes (Significancia Asíntota) es menor que α_1 se rechaza la hipótesis de trabajo (H_0) a nivel de significancia α_1
La hipótesis de trabajo es la que nos va aprobar.
Hemos trabajado con un nivel de confianza del 95% y un nivel de significancia **α** del 5%.

La tabla de contingencia cruzada muestra un resumen descriptivo de los datos observamos los resultados en el resumen de casos procesados entre estas dos variables cruzadas se aprecia 15 casos |que consideran que tienen en gran medida que consideran el Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS con Grado de autenticación del control del tráfico inalámbrico y 21 casos en Alguna medida haciendo un total de 36 casos y apenas 3 casos En poca Medida.

Tabla 24

Contingencia Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS * Grado de autenticación del control del tráfico inalámbrico

Resumen del procesamiento de los casos

	Casos					
	Válidos		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS * Grado de Autenticación	40	100,0%	0	0,0%	40	100,0%

		Valor	Error típ. asint.[a]	T aproximada[b]	Sig. aproximada
Nominal por nominal	Coeficiente de contingencia	,911			,003
Intervalo por intervalo	R de Pearson	,959	,013	20,898	,000[c]
Ordinal por ordinal	Correlación de Spearman	,928	,033	15,380	,000[c]
N de casos válidos		40			

Interpretación

Observamos que hay un R de Pearson del 95.9% y una alta correlación de Spearman del 92.8% entre las variables Seguridad de control y Grado de Autenticacion

Análisis Chi Cuadrado: Sistema de Seguridad de Control de Acceso con RADIUS con Grado de autenticación

Pruebas de chi-cuadrado

	Valor	Gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	195,333a	144	,003
Razón de verosimilitudes	122,042	144	,908
Asociación lineal por lineal	35,878	1	,000
N de casos válidos	40		

a. 169 casillas (100,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,03.

Toma de decisión:

Como el valor de significancia del estadístico es ρ = 0,003 es menor que α = 0,05 entonces existe suficiente evidencia estadística para rechazar la Hipótesis Nula y aceptamos la Hipótesis de Investigación : "Un sistema de seguridad de control con Acceso a RADIUS es significativo para determinar el grado de Autenticidad en el Control de tráfico inalámbrico"

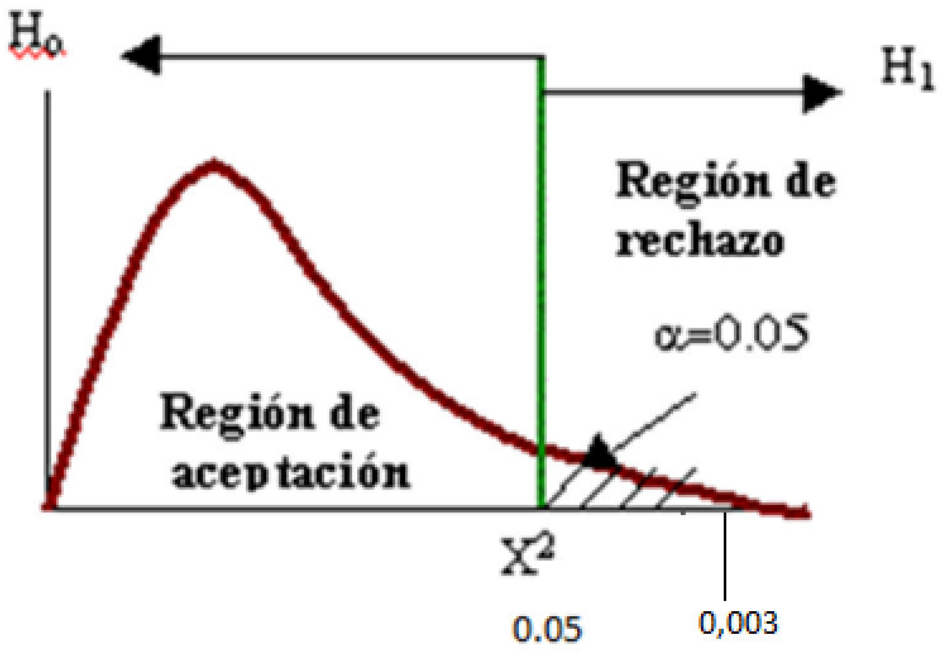


Tabla 25

Contingencia Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS * Grado de autorización del control del tráfico inalámbrico

Resumen del procesamiento de los casos

	Casos					
	Válidos		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS * Grado de Autorizacion	40	100,0%	0	0,0%	40	100,0%

Medidas simétricas

		Valor	Error típ. asint.[a]	T aproximada[b]	Sig. aproximada
Nominal por nominal	Coeficiente de contingencia	,948			,000
Intervalo por intervalo	R de Pearson	,948	,105	,851	,400[c]
Ordinal por ordinal	Correlación de Spearman	,858	,075	10,300	,000[c]
N de casos válidos		40			

Interpretación

Observamos que hay un R de Pearson del 94,8.% y una alta correlación de Spearman del 85.8% Seguridad de Control de Acceso y Grado de Autorizacion.

Análisis Chi Cuadrado: Sistema de Seguridad de Control de Acceso con RADIUS con Grado de autorización

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	358,000[a]	216	,000
Razón de verosimilitudes	159,235	216	,999
Asociación lineal por lineal	,729	1	,393
N de casos válidos	40		

a. 247 casillas (100,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,03.

Toma de decisión:

Como el valor de significancia del estadístico es ρ = 0,000 es menor que α = 0,05 entonces existe suficiente evidencia estadística para rechazar la Hipótesis Nula y aceptamos la Hipótesis de Investigación: "Un sistema de seguridad de control con Acceso a RADIUS es significativo para determinar el grado de Autorización en el Control de tráfico inalámbrico"

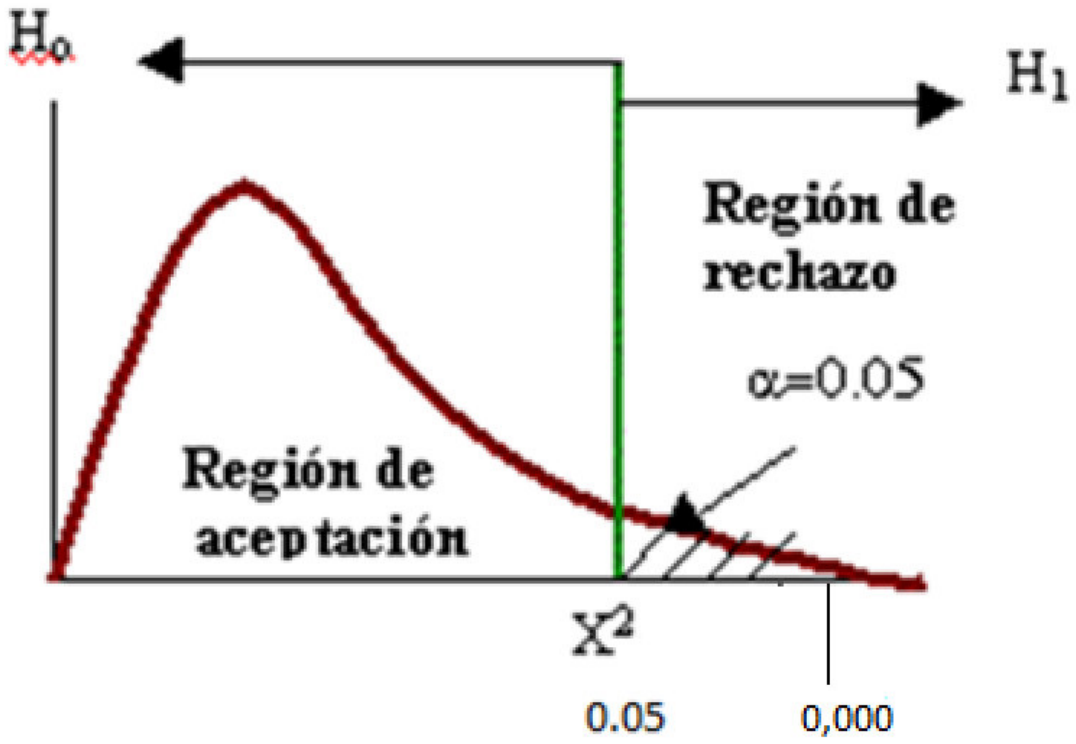


Tabla 26

Contingencia Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS * Modelo del Sistema de Administración para la mejora continua en la Gestión de Usuarios

Resumen del procesamiento de los casos

	Casos					
	Válidos		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS * Desarrollo Modelo de Administración	40	100,0%	0	0,0%	40	100,0%

Medidas simétricas

		Valor	Error típ. asint.[a]	T aproximada[b]	Sig. aproximada
Nominal por nominal	Coeficiente de contingencia	,948			,000
Intervalo por intervalo	R de Pearson	,979	,007	29,294	,000[c]
Ordinal por ordinal	Correlación de Spearman	,965	,015	22,627	,000[c]
N de casos válidos		40			

Interpretación

Observamos que hay un R de Pearson del 97,9.% y una alta correlación de Spearman del 96.5% entre las variables Seguridad de Control y Modelo de Administración.

Análisis Chi Cuadrado: Sistema de Seguridad de Control de Acceso con RADIUS y un Modelo del Sistema de Administración para la mejora continua en la Gestión de Usuarios

Pruebas de chi-cuadrado

	Valor	Gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	351,611[a]	252	,000
Razón de verosimilitudes	158,694	252	1,000
Asociación lineal por lineal	37,346	1	,000
N de casos válidos	40		

a. 286 casillas (100,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,03.

Toma de decisión:

Como el valor de significancia del estadístico es ρ = 0,000 es menor que α = 0,05 entonces existe suficiente evidencia estadística para rechazar la Hipótesis Nula y aceptamos la Hipótesis de Investigación: "Desarrollo de un Modelo de Sistema de Administración para la mejora continua en la Gestión de Usuarios en el Control de Trafico Inalámbrico mejora su performance."

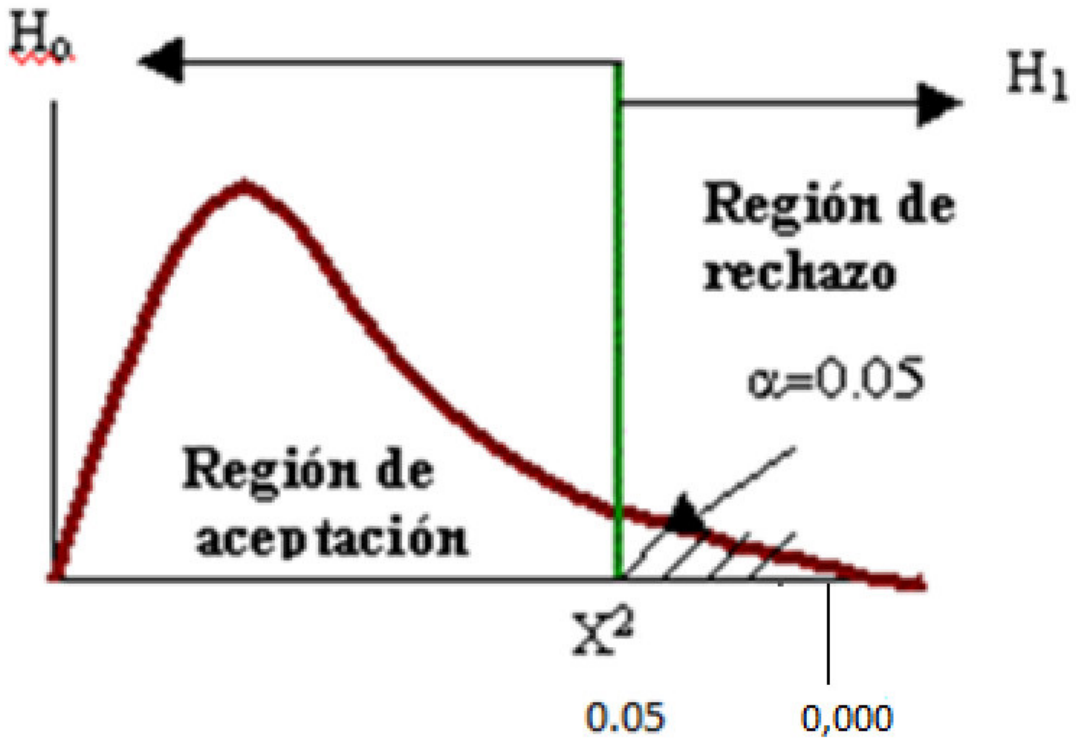


Tabla 27

Desarrollo e Implementación de un Sistema de Seguridad de Control de Acceso con RADIUS produce efectos que determina el Grado de Autenticación y Autorización en el Control de tráfico Inalámbrico

Resumen del procesamiento de los casos

	Casos					
	Válidos		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS * Grado de Autenticación	40	100,0%	0	0,0%	40	100,0%
Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS * Grado de Autorización	40	100,0%	0	0,0%	40	100,0%
Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS * Desarrollo Modelo de Administración	40	100,0%	0	0,0%	40	100,0%

Medidas simétricas

		Valor	Error típ. asint.[a]	T aproximada[b]	Sig. aproximada
Nominal por nominal	Coeficiente de contingencia	,911			,003
Intervalo por intervalo	R de Pearson	,959	,013	20,898	,000[c]
Ordinal por ordinal	Correlación de Spearman	,928	,033	15,380	,000[c]
N de casos válidos		40			

Interpretación

Hay una excelente R de Pearson del 95.9% y una muy buena correlación de Spearman de 92,8% entre las variables Grado de Autenticación, Grado de Autorización y Desarrollo del Modelo de Administración.

Análisis Chi Cuadrado: Entre el Grado de Autenticación Autorización y Modelo de Sistema de Gestion.

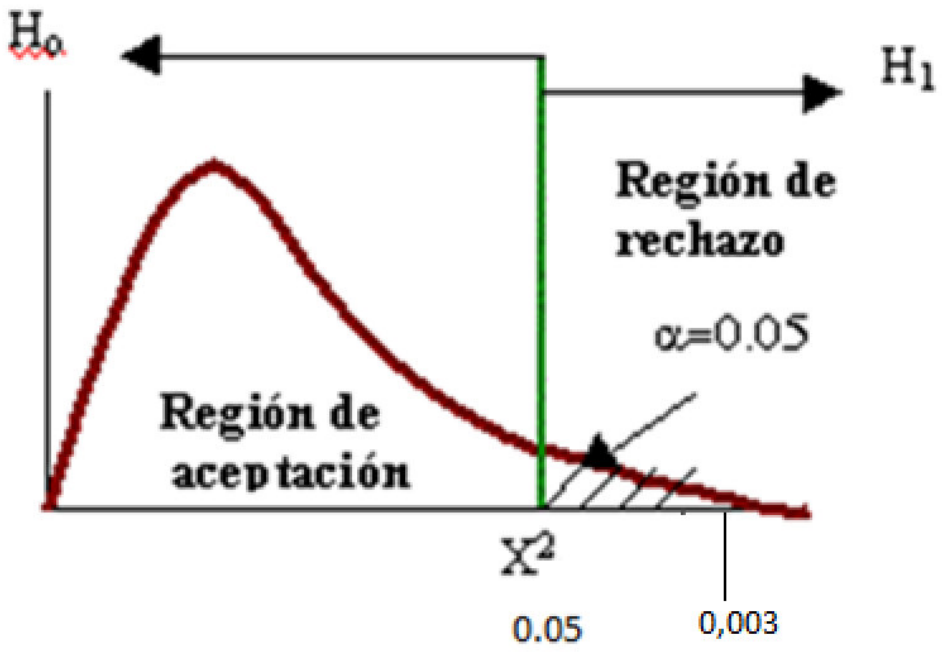
Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	195,333[a]	144	,003
Razón de verosimilitudes	122,042	144	,908
Asociación lineal por lineal	35,878	1	,000
N de casos válidos	40		

a. 169 casillas (100,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,03.

Toma de decisión:

Como el valor de significancia del estadístico es ρ = 0,003 es menor que α = 0,05 entonces existe suficiente evidencia estadística para rechazar la Hipótesis Nula y aceptamos la Hipótesis de Investigación: "Desarrollo e Implementación de un Sistema de Seguridad de Control de Acceso con RADIUS produce efectos que determina el Grado de Autenticación y Autorización en el control de Trafico Inalámbrico."



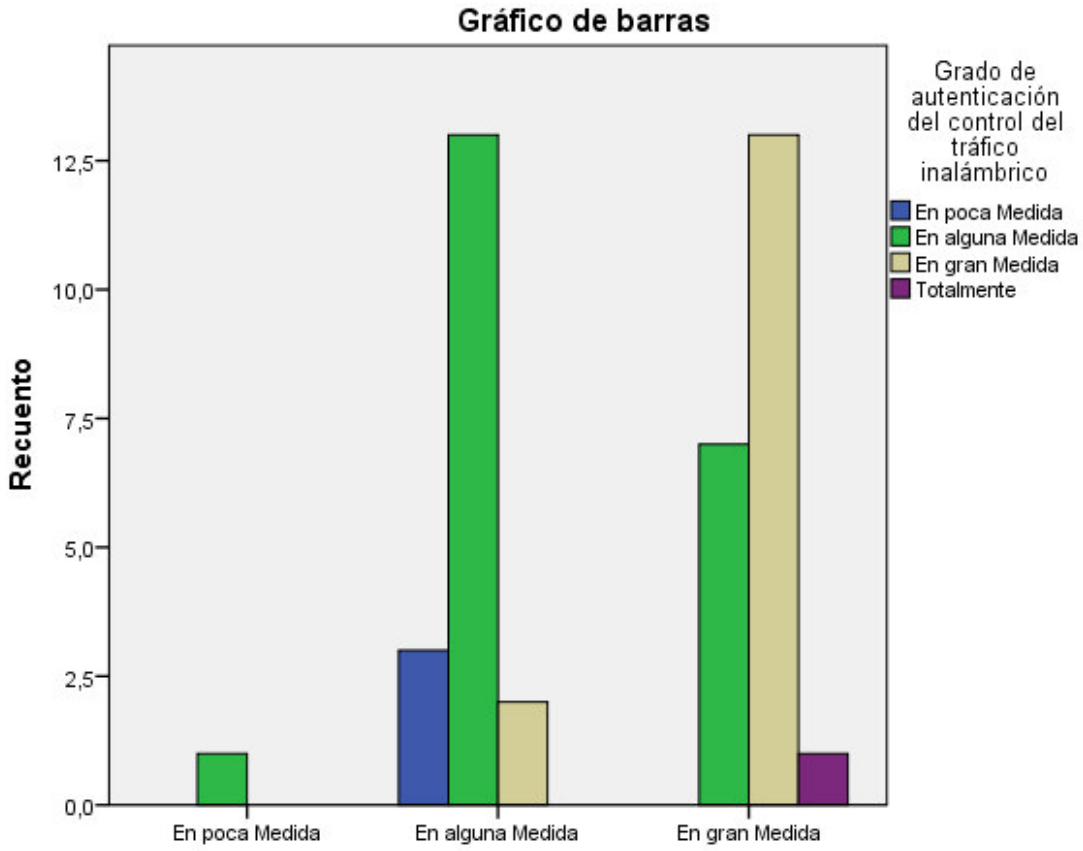


Figura 33: **Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS.**

Fuente. IGP-Encuesta virtual

Tabla 25.
Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	14,857[a]	6	,021
Razón de verosimilitudes	17,468	6	,008
Asociación lineal por lineal	12,164	1	,000
N de casos válidos	40		

a. 8 casillas (66,7%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,03.

Fuente: Resultados del Chi-cuadrado de Pearson con SPSS 20

Fuente. Datos tomados de - Encuesta Virtual IGP

- Haciendo la comparación con el Valor 0,021 de la significancia asíntota se observa que es menor que 0.05, asumiendo que **α** se

acepta la hipótesis de trabajo y se rechaza la hipótesis nula, es decir que el **Diseño de un sistema de seguridad de control de acceso con RADIUS es significativo para determinar el grado de autenticidad en el control del tráfico inalámbrico**

Tabla 26.

Resumen del procesamiento de los casos de Variables Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS y Grado de autenticación del control del tráfico inalámbrico

	Casos					
	Válidos		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS * Grado de autenticación del control del tráfico inalámbrico	40	100,0%	0	0,0%	40	100,0%

Fuente. Datos arrojados del SPSS 20 para hallar los casos

4.7.2 Contrastación de la Segunda Hipótesis Específica.

- H_0: El empleo de un sistema de seguridad del control de acceso con Radius No mide significativamente el grado de autorización del control del tráfico inalámbrico.
- H_1: El empleo de un sistema de seguridad del control de acceso con Radius mide significativamente el grado de autorización del control del tráfico inalámbrico.

Si el ***p*** valor asociado al estadístico de contrastes (Significancia Asíntota) es menor que α_1 se rechaza la hipótesis de trabajo (H_0) a nivel de significancia α_1

La hipótesis de trabajo es la que nos va aprobar.

Hemos trabajado con un nivel de confianza del 95% y un nivel de significancia **α** del 5%.

La tabla de contingencia cruzada muestra un resumen descriptivo de los datos observamos los resultados en el resumen de casos procesados entre estas dos variables cruzadas se aprecia 21 casos que consideran que tienen en gran medida que consideran el Grado de autorización del control del tráfico inalámbrico con el Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS y 18 casos en Alguna medida haciendo un total de 39 casos y apenas 1 caso En poca Medida.

Recuento

		Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS			Total
		En poca Medida	En alguna Medida	En gran Medida	
Grado de autorización del control del tráfico inalámbrico	En poca Medida	0	1	0	1
	En alguna Medida	1	10	8	19
	En gran Medida	0	7	13	20
Total		1	18	21	40

Fuente. Resultados mostrados por el programa SPSS 20 de las pruebas de contingencia

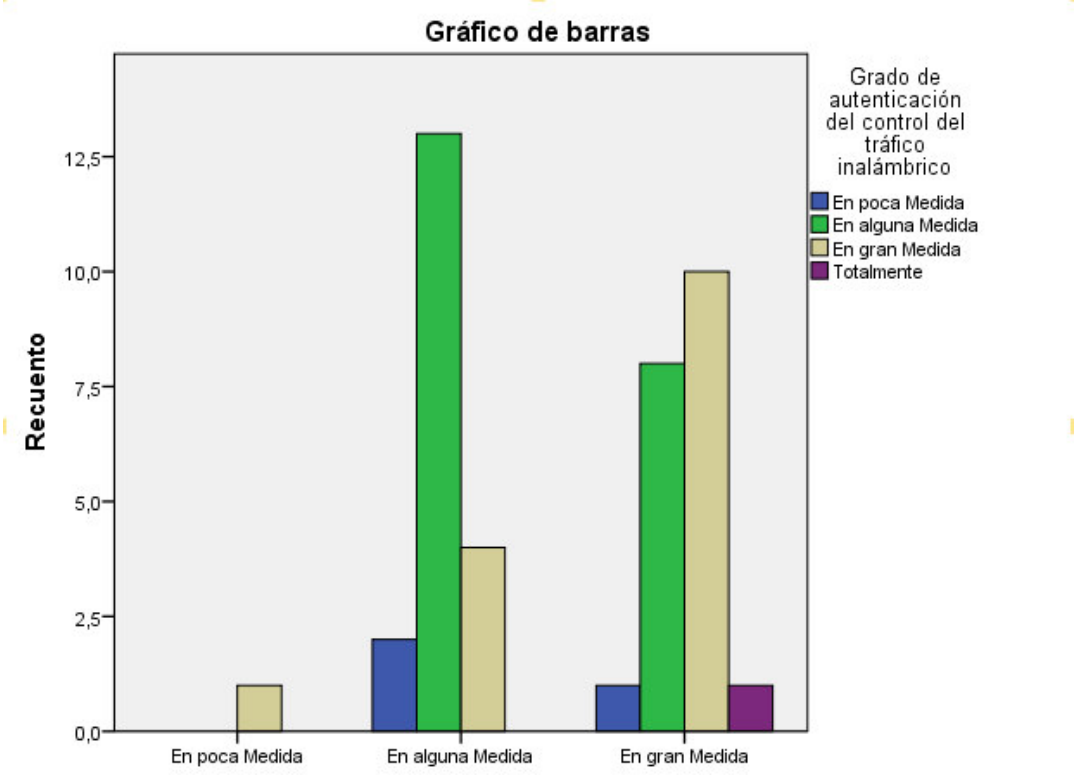


Figura 34: **Grado de Autorización del control de Trafico Inalámbrico**

Fuente: IGP-Encuesta virtual

Tabla 27.

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	3,979[a]	4	,0409
Razón de verosimilitudes	4,723	4	,317
Asociación lineal por lineal	3,325	1	,068
N de casos válidos	40		

a. 5 casillas (55,6%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,03.

Fuente. Resultados mostrados por el programa SPSS 20 de las pruebas Chi cuadrado

- Haciendo la comparación con el Valor 0,0409 de la significancia asíntota se observa que es menor que 0.05, asumiendo que **α** se acepta la hipótesis de trabajo y se rechaza la hipótesis nula, es decir que el **empleo de un sistema de seguridad del control de acceso con RADIUS mide significativamente el grado de autorización del control del tráfico inalámbrico.**

Tabla 28.

Resumen del procesamiento de los casos

	Casos					
	Válidos		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Grado de autorización del control del tráfico inalámbrico * Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS	40	100,0%	0	0,0%	40	100,0%

Fuente. Resultados del programa SPSS 20 de las pruebas procesamiento de casos

4.7.3 Contrastación de la Hipótesis General

- H_0: Un Sistema de Seguridad de Control de Acceso con RADIUS No produce efectos que determina el grado de autenticación y autorización en el control de tráfico inalámbrico.
- H_1: Un Sistema de Seguridad de Control de Acceso con RADIUS produce efectos que determina el grado de autenticación y autorización en el control de tráfico inalámbrico..

Si el ***p*** valor asociado al estadístico de contrastes (Significancia Asíntota) es menor que α_1 se rechaza la hipótesis de trabajo (H_0) a nivel de significancia α_1

La hipótesis de trabajo es la que nos va aprobar.

Hemos trabajado con un nivel de confianza del 95% y un nivel de significancia **α** del 5%.

La tabla de contingencia cruzada muestra un resumen descriptivo de los datos observamos los resultados en el resumen de casos procesados entre estas dos variables cruzadas se aprecia que 15 casos que consideran que tienen en gran medida que consideran que Un Sistema de Seguridad de Control de Acceso con RADIUS produce efectos que determina el grado de autenticación y autorización en el control de tráfico inalámbrico y 21 casos en Alguna medida, Totalmente 1 caso y apenas 3 casos En poca Medida.

Tabla 29.

Contingencia Grado de autorización del control del tráfico inalámbrico * Grado de autenticación del control del tráfico inalámbrico.

Recuento

Grado de autorización del control del tráfico inalámbrico		Grado de autenticación del control del tráfico inalámbrico				Total
		En poca Medida	En alguna Medida	En gran Medida	Totalmente	
Grado de autorización del control del tráfico inalámbrico	En poca Medida	0	0	1	0	1
	En alguna Medida	2	13	4	0	19
	En gran Medida	1	8	10	1	20
Total		3	21	15	1	40

Fuente. Resultados mostrados por el programa SPSS 20

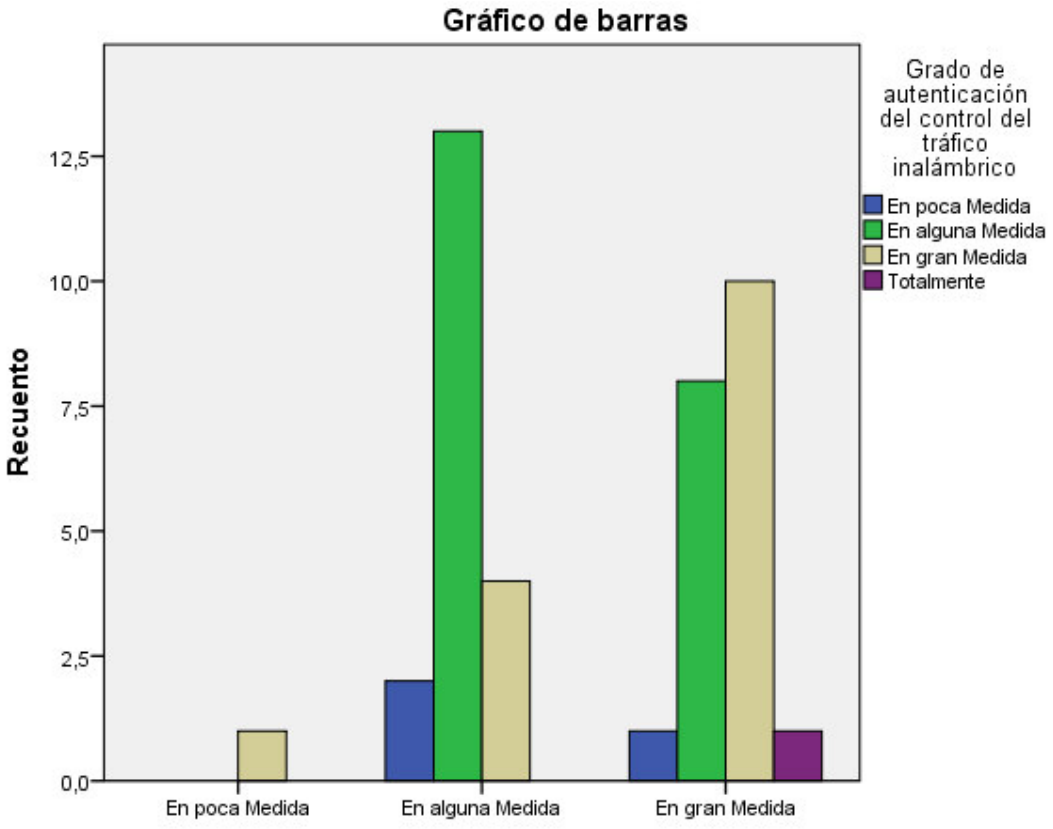


Figura 35: **Grado de Autorización del control del Tráfico inalámbrico**

Fuente. IGP-Encuesta virtual

- Haciendo la comparación con el Valor 0,0344 de la significancia asíntota se observa que es menor que 0.05, asumiendo que **α** se acepta la hipótesis de trabajo y se rechaza la hipótesis nula, es decir

que **Un Sistema de Seguridad de Control de Acceso con RADIUS produce efectos que determina el grado de autenticación y autorización en el control de tráfico inalámbrico**

Tabla 30.

Pruebas de chi-cuadrado

	Valor	Gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	6,757[a]	6	,0344
Razón de verosimilitudes	7,564	6	,272
Asociación lineal por lineal	2,137	1	,144
N de casos válidos	40		

a. 8 casillas (66.7%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es .03.

Fuente. Resultados mostrados por el programa SPSS 20

Tabla 31.

Resumen del procesamiento de los casos

	Casos					
	Válidos		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Grado de autorización del control del tráfico inalámbrico * Grado de autenticación del control del tráfico inalámbrico	40	100,0%	0	0,0%	40	100,0%

*Fuente.*Resultados mostrados por el programa SPSS 20

4.8. Presentación de Resultados

OBSERVACIONES A LA SUSTENTACION

4.8.1 Infraestructura inalámbrica inicial del Instituto Geofísico del Perú

El instituto geofísico del Perú se ubica en Calle Calatrava, 216, La Molina 15023, Lima – Perú. (Sede de Camacho), la red inalámbrica presentaba las siguientes características antes de la ejecución del proyecto:

- Contaba con cinco (05) equipos puntos de acceso inalámbricos para irradiar de red a todas las oficinas de la Sede Principal ubicada en el Distrito de Ate, encontrándose ubicado en los siguientes ambientes: Sala de Usos Multiples (SUM), Biblioteca de la sede Principal (Mayorazgo), Sub dirección de ciencias de la tierra solida – SDCTS, Sub dirección de Ciencias de la Atmosfera de la Hidrosfera – SDCAH y Alta Dirección.
- Utilizaba un protocolo de acceso de seguridad WPA2, el cual es un protocolo basado en estándares de seguridad inalámbrica 802.11i.
- Las contraseñas de acceso a los puntos inalámbricos eran de conocimiento para todos los usuarios del Instituto Geofísico del Perú, no se contaba con restricción para bloquear eventos atípicos en la red Inalámbrica de la Institución,
- No se contaba con una plataforma de directorio a nivel de los equipos de red que jerarquice a los usuarios para el acceso a la red inalámbrica.
- La contabilidad de los accesos a la red inalámbrica solo era verificado por los eventos internos de cada equipo inalámbrico.
- Los usuarios se limitaban al acceso inalámbrico dentro de la Institución.

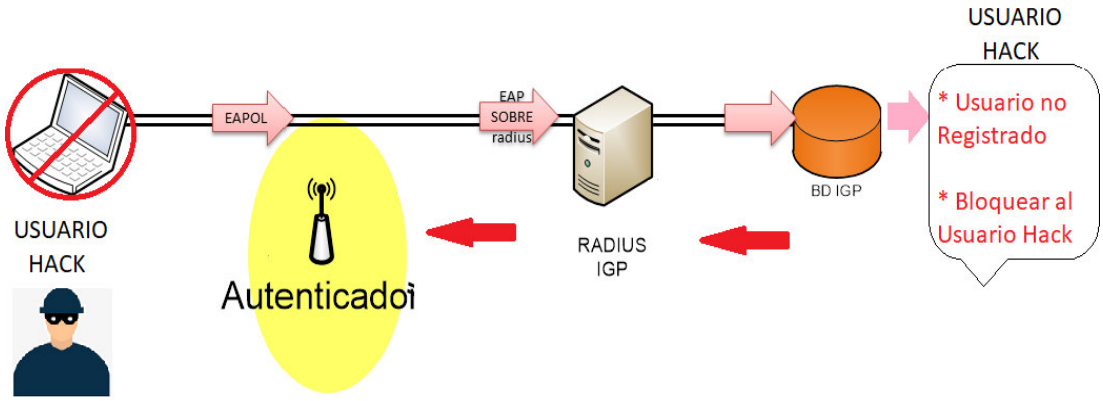
4.8.2 Evidencias de Mejora con la Implementación del desarrollo de la Investigación a través del servicio de RADIUS y el Servidor LDAP

- La sede Principal ubicada en el distrito de Ate se potencio en un Modelo de Sistema Administración para la mejora continua en la gestión de usuarios en el control de tráfico Inalámbrico con las siguientes sedes a nivel nacional:

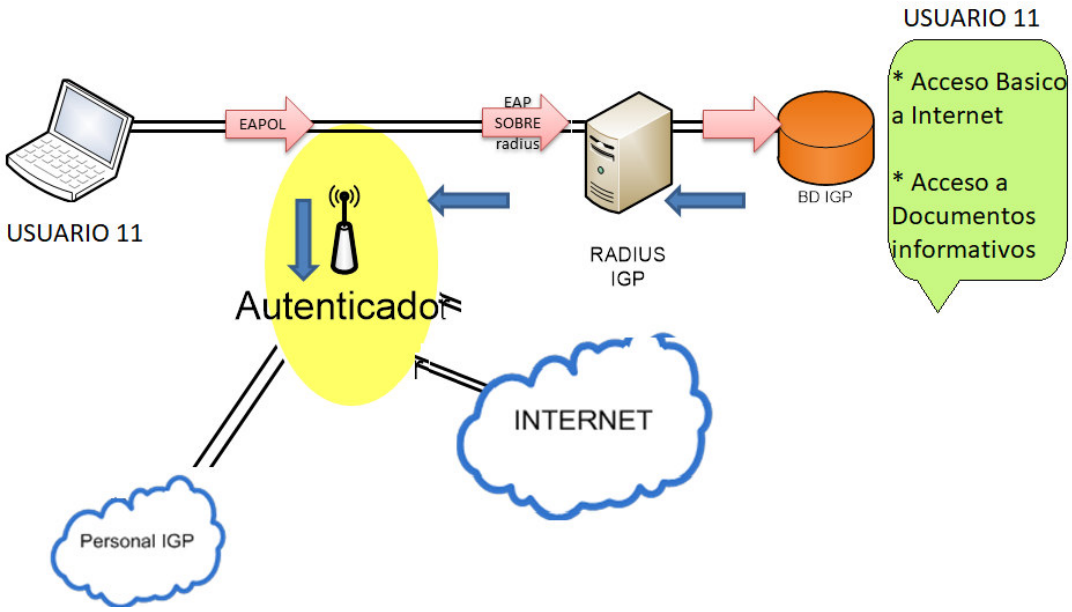
ITEM	SEDE	AREA
1	Jicamarca	• Radio Observatorio – ROJ (Implementación de Autenticación y Autorización inalámbrica)
2	Mayorazgo	• Sub dirección de Ciencias de la Atmosfera de la Hidrosfera – SDCAH (Implementación de Autenticación y Autorización inalámbrica) • Sub Dirección de Geofísica y Sociedad – SDGYS (Implementación de Autenticación y Autorización inalámbrica)
3	Camacho	• Sub dirección de Redes Geofísicas – SDRG (Implementación de Autenticación y Autorización inalámbrica) • Sub dirección de ciencias de la tierra solida – SDCTS (Implementación de Autenticación y Autorización inalámbrica)
4	Huancayo	• Observatorio de Huancayo – OHY (Implementación de Autenticación y Autorización inalámbrica)
5	Arequipa	• Observatorio Vulcanológico del Sur – OVS (Implementación de Autenticación y Autorización inalámbrica)

- Se utilizó el protocolo de acceso de seguridad EAP y RADIUS para la red inalámbrica.

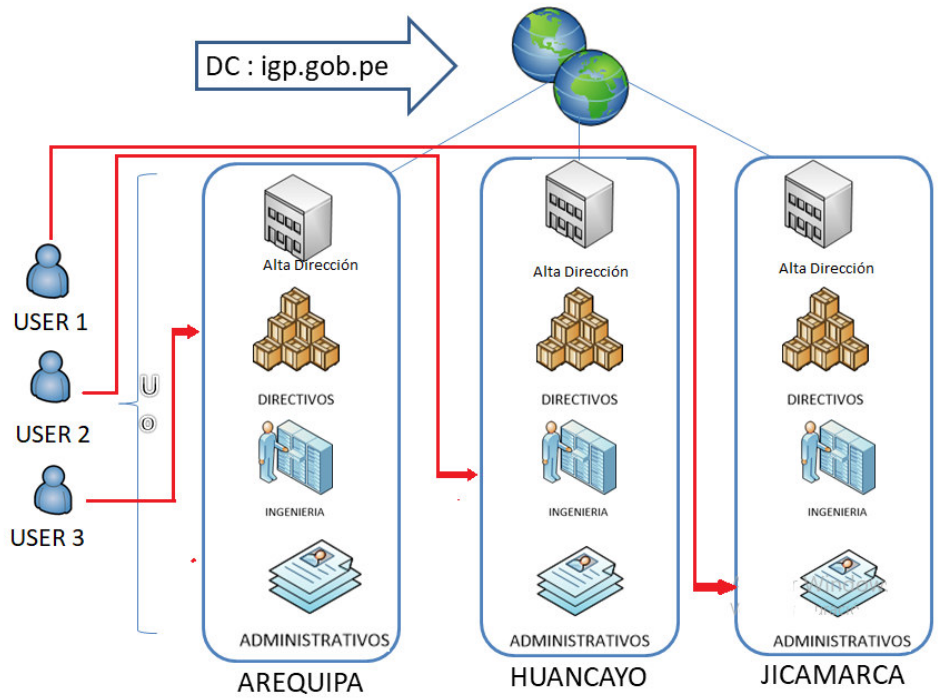
- Con relación al Grado de Autenticación en el control de tráfico Inalámbrico en el Instituto Geofísico del Perú (IGP), cada usuario para acceder a la red inalámbrica utiliza como identificador su cuenta de correo electrónico, el cual ha sido registrado en el Directorio Activo del servicio LDAP



- Con relación al Grado de Autorización en el control de tráfico Inalámbrico, el Sistema RADIUS y LDAP otorga según el perfil de usuario los permisos a los servicios Internos como los externos de la Institución.



- Con respecto a Desarrollar el modelo de Sistema Administrativo y Gestión de Usuarios en el Control de Tráfico Inalámbrico, la contabilidad al acceso inalámbrico se verifica con la herramienta de código abierto OPENLDAP que utiliza el protocolo LDAP (phpLdapadmin) el cual es un protocolo a nivel de aplicación que permite el acceso al directorio Activo de la Institución, el cual se encuentra distribuido para buscar diversa información en el entorno de red Institucional, a fin de mejorar los permisos de Autenticación y Autorización en el control del tráfico Inalámbrico del Instituto Geofísico del Perú - IGP



- Con respecto al “Desarrollar e Implementar los efectos que produce un Sistema de seguridad de Control de Acceso con RADIUS en el grado de Autenticación y Autorización del control de tráfico inalámbrico de información, actualmente el servicio implementado permite a los miembros de la institución poder acceder a internet en cualquier institución en el mundo que utilice la aplicación eduroam.

CAPITULO V: IMPACTOS

5.1 Propuesta de la Solución.

5.1.1 Objetivo

Con el análisis de este sistema de control de seguridad, el servicio basado en la autenticación y autorización de los usuarios en el acceso a la red inalámbrica de la Institución, se desarrolló un modelo de Sistema Administrativo para la mejora continua en la gestión de los usuarios en el control de tráfico inalámbrico para la mejora performance, quienes al pertenecer a este servicio podrán movilizarse en otras instituciones que cuenten con el mismo servicio el cual será basada en el Protocolo RADIUS, con el uso de una autenticación AAA y el protocolo LDAP para la gestión administrativa de los usuarios.

5.1.2 Descripción

El modelo de gestión utiliza una herramienta en código abierto que usa el protocolo Ldap, esta herramienta viene hacer una base de datos donde se registraran los usuarios, los cuales serán representados mediante un identificador que para nuestro caso será se designó el correo institucional de los usuarios, esto permitirá la jerarquización y correspondencia de cada usuario.

El servicio basado en el protocolo RADIUS incluirá el servicio eduroam (contracción de education roaming), se basa en IEEE 802.1X y una jerarquía de servidores proxy RADIUS, el rol de la jerarquía RADIUS es reenviar las credenciales de usuarios a la institución local de los usuarios, donde ellos pueden ser verificados y validados.

Cuando un usuario solicita autenticación, el dominio del usuario determina donde es enrutada la solicitud, el dominio es un sufijo del nombre de usuario,

delimitado con “@”, y es derivado del nombre de dominio DNS de la organización.

Cada institución que desee participar en eduroam, conecta su servidor RADIUS institucional al servidor RADIUS Top-Level Nacional (NTLR) del país donde la institución se localiza. El NTLR es normalmente operado por una NREN del país, estos Servidores Country-Level tienen una completa lista de las instituciones eduroam participantes en este país. Esto es suficiente para garantizar el roaming nacional, para roaming internacional, es necesario un servidor RADIUS Top-Level Regional para “reenviar” la solicitud de los usuarios al país correcto.

Originalmente habían dos regiones principales donde se desarrolló eduroam: Europa y Asia-Pacífico. Ahora: Norte América, Latino América y África. en Europa, el servidor RADIUS Top-Level (ETLR) es operado por: Dutch NREN (SURFnet) y la Danish NREN (UNI-C), en Asia-Pacífico, el servidor RADIUS Top-Level (APTLR) es operado por la NREN de Australia (AARNet) y por la Universidad de Hong Kong.

En Latino América, el RADIUS Proxy Server (RPS-LA) es operado por INICTEL-UNI (RAAP).

5.1.3 Instalación del Servidor RADIUS y con la aplicación eduroam:

- Instalación de paquetes y librerías necesarias
- Creando la solicitud de un certificado digital para enviárselo a la Autoridad Certificadora
- Generación de claves GPG (GNU Privacy Guard) para el intercambio de secretos entre los servidores RADIUS. Se recomienda usar una PC Linux con entorno gráfico
- Configurar las claves locales y remotas para los clientes y especificar el realm local correspondiente al servidor RADIUS.
- Configurar el archivo de usuarios del servidor Radius Local.

5.1.4 LDAP y LOGs

- Servidor Ldap bajo una plataforma phpLDAPadmin actúa como un Directorio Activo. La configuración se realiza en el servidor RADIUS en: (/etc/freeradius/modules/ldap)

```
ldap {
        #
        # Note that this needs to match the name in the LDAP
        # server certificate, if you're using ldaps.
        server = 10.10.40.18
        #identity = "cn=admin,o=My Org,c=UA"
        #password = mypass
        basedn = "ou=USUARIOS,dc=igp,dc=gob,dc=pe"
        filter  =  "(uid=%{%{Stripped-User-Name}:-%{User-
Name}})"
        base_filter = "(objectclass=radiusprofile)"
```

Figura 36: Configuración del Servidor LDAP en el archivo de configuración del servidor RADIUS.

Fuente: IGP

- Al asociar el servidor Ldap al servidor RADIUS nos muestra la siguiente plataforma en web

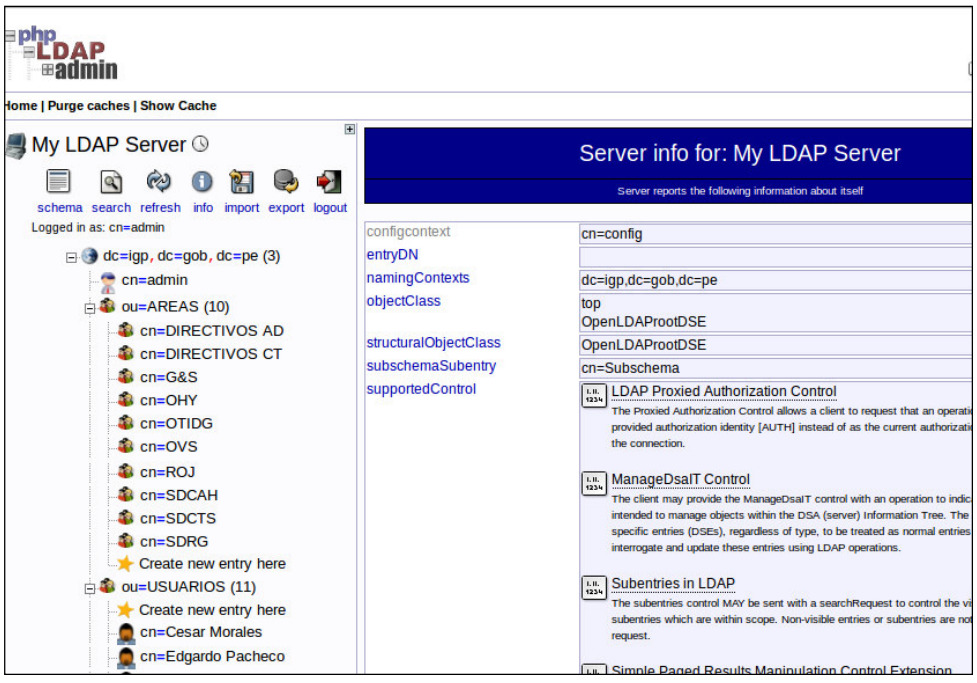


Figura 37: Plataforma phpLDAPadmin para la administración de la Jerarquía de usuarios.

Fuente. IGP

- Evento de usuario rechazado

```
rad_recv: Access-Request packet from host 10.10.10.1 port 45772, id=104, length=85
Sending duplicate proxied request to home server 127.0.0.1 port 1830 - ID: 129
Sending Access-Request of id 129 to 127.0.0.1 port 1830
   User-Name = "elvis.espinoza@igp.gpb.pe"
   User-Password = "pass"
   NAS-IP-Address = 127.0.1.1
   NAS-Port = 0
   Message-Authenticator = 0x00000000000000000000000000000000
   Proxy-State = 0x313034
Waking up in 25.0 seconds.
rad_recv: Access-Request packet from host 10.10.10.1 port 45772, id=104, length=85
Sending duplicate proxied request to home server 127.0.0.1 port 1830 - ID: 129
Sending Access-Request of id 129 to 127.0.0.1 port 1830
   User-Name = "elvis.espinoza@igp.gpb.pe"
   User-Password = "pass"
   NAS-IP-Address = 127.0.1.1
   NAS-Port = 0
   Message-Authenticator = 0x00000000000000000000000000000000
   Proxy-State = 0x313034
Waking up in 19.9 seconds.
ASSERT FAILED event.c[1181]: "We do not have threads, but the request is marked as queued or running in a child thread" == NULL
```

Figura38: Eventos del sistema: Usuario rechazado.

Fuente. IGP

- Eventos de acceso y permiso al sistema

```
Sending Access-Request of id 69 to 127.0.0.1 port 1812
   User-Name = "user@igp.gob.pe"
   User-Password = "pass"
   NAS-IP-Address = 127.0.1.1
   NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=69, length=20

Sending Access-Request of id 72 to 127.0.0.1 port 1812
   User-Name = "eespinoza@igp.gob.pe"
   User-Password = "pass"
   NAS-IP-Address = 127.0.1.1
   NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=72, length=20

Sending Access-Request of id 25 to 127.0.0.1 port 1812
   User-Name = "jvillegas@igp.gob.pe"
   User-Password = "pass"
   NAS-IP-Address = 127.0.1.1
   NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=25, length=20

Sending Access-Request of id 32 to 127.0.0.1 port 1812
   User-Name = "jose.machare@igp.gob.pe"
   User-Password = "pass"
   NAS-IP-Address = 127.0.1.1
   NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=32, length=20

Sending Access-Request of id 43 to 127.0.0.1 port 1812
   User-Name = "dscipion@igp.gob.pe"
   User-Password = "pass"
   NAS-IP-Address = 127.0.1.1
   NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=43, length=20

Sending Access-Request of id 43 to 127.0.0.1 port 1812
   User-Name = "richardqa@inictel-uni.edu.pe"
   User-Password = "pass"
   NAS-IP-Address = 127.0.1.1
   NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=43, length=20

Sending Access-Request of id 78 to 127.0.0.1 port 1812
   User-Name = "jquiroz@inictel-uni.edu.pe"
   User-Password = "pass"
   NAS-IP-Address = 127.0.1.1
   NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=78, length=20
```

Figura39: Eventos del sistema: Acceso y Autorización a los usuarios.

Fuente. IGP

5.1.5 Servidor Redes Inalámbricas IEEE 802.11

- Borrar todos los archivos encontrados en la carpeta /etc/freeradius/certs/
- Copiar los archivos creados en el anteriormente en la ruta /etc/freeradius/certs
- Configurar los clientes de su servidor RADIUS Local

```
proxy server {
 default_fallback      = yes
}
home_server ftlr {
        type                    = auth+acct
        ipaddr                  = 190.12.88.20
        port                    = 1812, 1813
        secret                  = <clave-compartida>
        response_windows        = 20
        zombie_period           = 40
        revive_interval         = 60
        status_check            = status-server
        check_interval          = 30
        num_answers_to_alive    = 3
}
home_server_pool EDUROAM-FTLR {
        type = fail-over
        home_server = ftlr
}
realm <Institución>.<gob|edu>.pe {
        type = radius
        authhost = LOCAL
        accthost = LOCAL
}
realm LOCAL {
nostrip
}
realm null {
nostrip
}
realm "~.+$" {
        pool = EDUROAM-FTLR
        nostrip
}
```

Figura 40: Configuración del servidor RADIUS.

Fuente. INICTEL

5.1.6 Funcionamiento y Políticas

Para el funcionamiento usaremos un ejemplo veremos como un usuario llamado “Lucas” que pertenece a IGP y se encuentra en una entidad “Externa” obtiene el acceso a red a través del proceso de autenticación y autorización de eduroam:

- El dispositivo móvil de Lucas se une a SSID eduroam
- El cliente sobre el dispositivo móvil de Lucas envía una solicitud de conexión a la red eduroam de la entidad “externa” como lucas@igp.gob.pe
- El servidor local RADIUS de la entidad “Externa” (que está conectado a la infraestructura inalámbrica de “Externa”) reconoce que el dominio de Lucas (@igp.gob.pe) no es local, por lo que reenvía la solicitud al servidor RADIUS nacional.
- El servidor RADIUS nacional envía la solicitud al destino apropiado, dominio igp.gob.pe
- El servidor RADIUS de IGP, envía un certificado de desafío (certificate challenge) de regreso a Lucas. Este es el paso que permitirá a Lucas estar seguro que el SSID eduroam de la entidad “Externa” es un miembro de confianza de la red de eduroam.
- Si el certificado fue cargado previamente en el dispositivo de Lucas (un importante paso en el proceso de eduroam), el dispositivo aceptará el certificado y establece un túnel encriptado SSL/TLS entre el dispositivo de Lucas y el servidor RADIUS home (origen) de la institución de Lucas - IGP. Si el dispositivo móvil de Lucas no reconoce el certificado, a Lucas se le pedirá que acepte o rechace el certificado. En todos los casos, el certificado mostrará el nombre común (por ejemplo: eduroam-radius.igp.edu). Lucas no debería aceptar un Certificado con un nombre desconocido (por ejemplo: verdad.com).
- Ahora que se ha establecido el túnel encriptado entre el dispositivo de Lucas y el servidor RADIUS de IGP, las credenciales de Lucas son

pasadas a través del túnel encriptado SSL/TLS entre el dispositivo de Lucas y el servidor RADIUS de IGP para la verificación. Este paso de autenticación permite al servidor RADIUS ser conectado al Servicio de Directorio de la institución.

- Sobre la autenticación exitosa, el servidor RADIUS de IGP envía un Access-accept y algún material clave a la infraestructura de la entidad "Externa" (fuera del túnel SSL) y algún material clave privado a pepe (dentro del túnel).
- La infraestructura inalámbrica eduroam de la entidad "Externa" negocia con el dispositivo de pepe el intercambio de la clave de encriptación para permitir el acceso a la red y habilitar la encriptación entre el dispositivo de Lucas y los puntos de acceso inalámbrico de "Externa".
- Lucas ahora puede conectarse a SSID eduroam en "Externa" y disfrutar de la conectividad autenticada y encriptada entre su dispositivo y la red inalámbrica de "Externa".

Políticas

- El acceso a la red inalámbrica adherida al servicio eduroam (SSID: eduroam) está disponible para todo el personal de Investigadores del IGP, y para los usuarios cuya institución está adherida a la iniciativa eduroam
- Se entiende que el uso está orientado a ofrecer la facilidad de movilidad, objetivo de la iniciativa.
- Las cuentas de acceso al servicio eduroam es personal e intransferible, no pudiendo ser cedido a otras personas.
- Toda actividad realizada usando su cuenta de acceso, es de responsabilidad de propietario de la cuenta. No habiendo responsabilidad de IGP como consecuencia de uso del servicio.

Esquema de Funcionamiento de autenticación del servicio eduroam

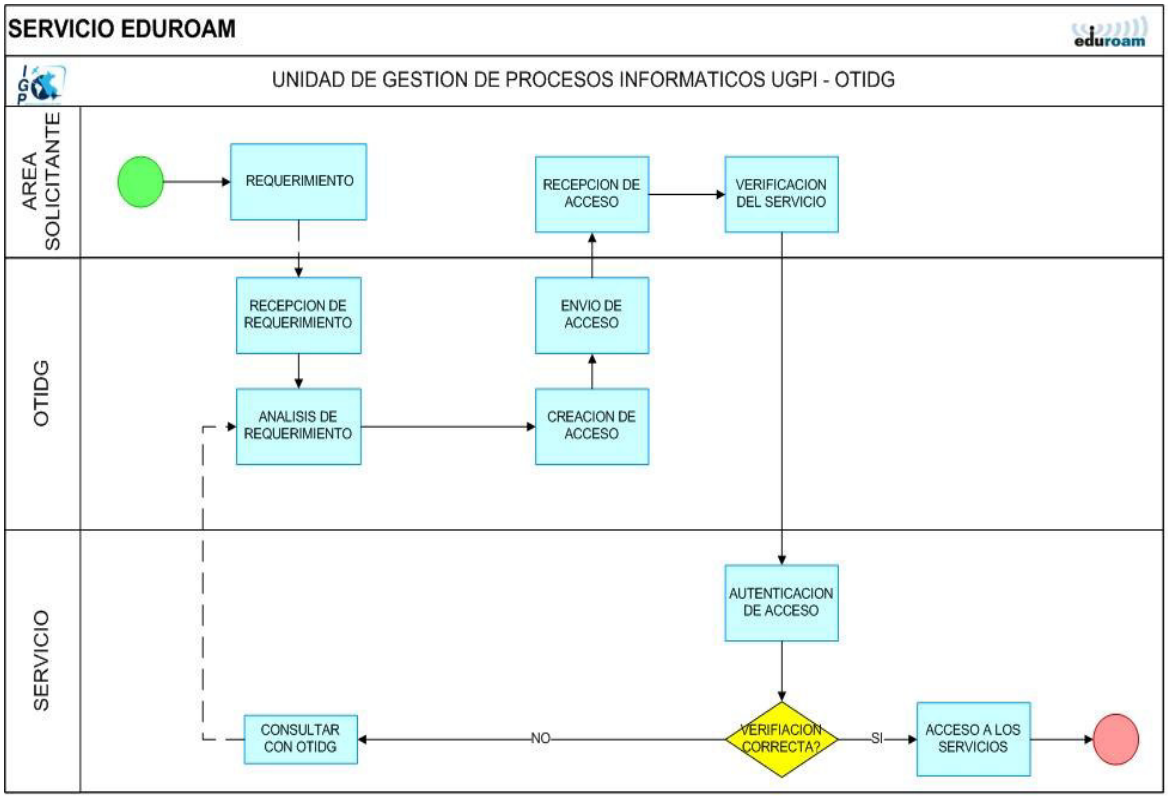


Figura 38: **Diagrama de Flujo – Interno del proceso de gestión con el servicio eduroam**

Fuente. IGP

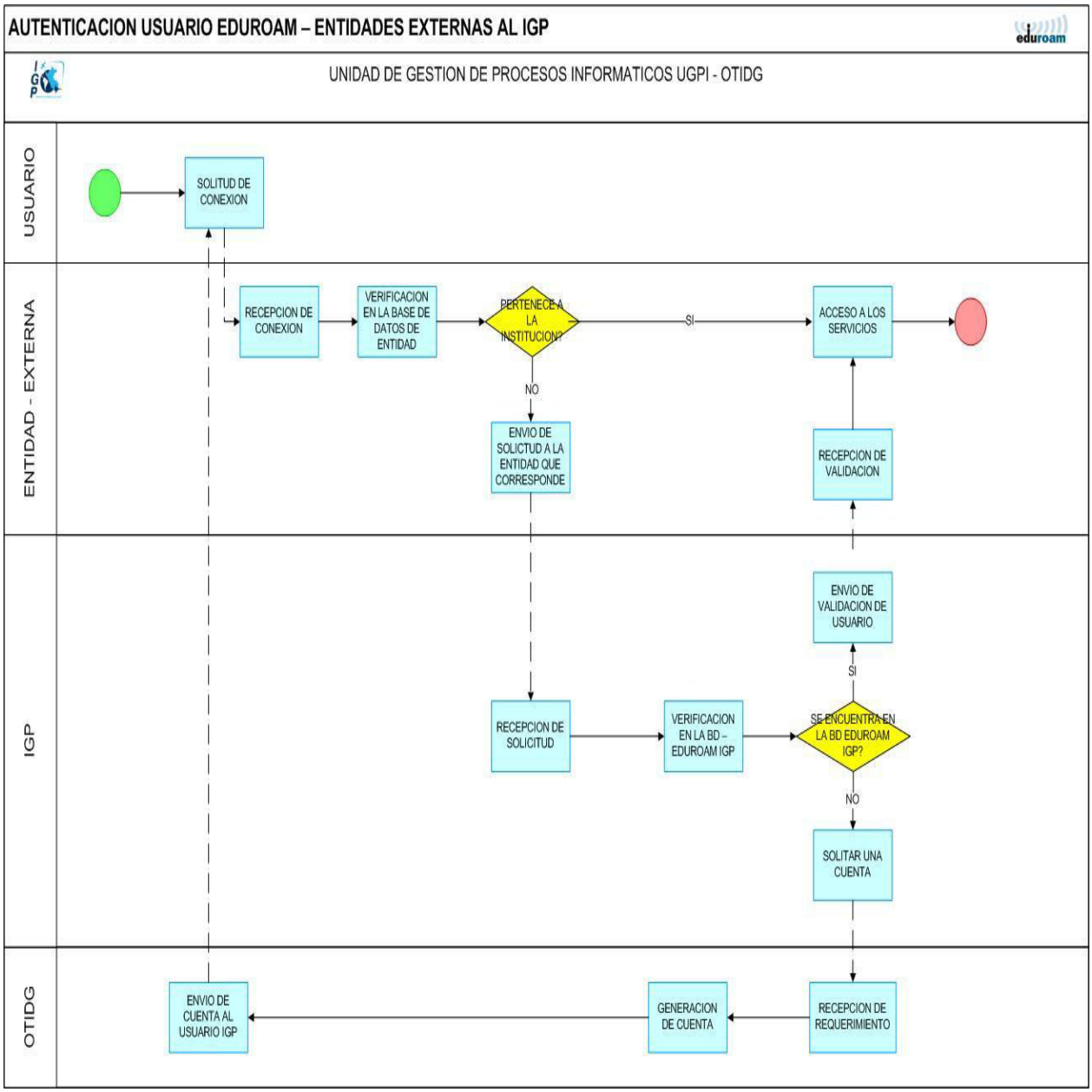


Figura 39: **Diagrama de Flujo – Externo del proceso de gestión con el servicio eduroam**

Fuente. IGP

Esquema de autenticación de la propuesta RADIUS con eduroam

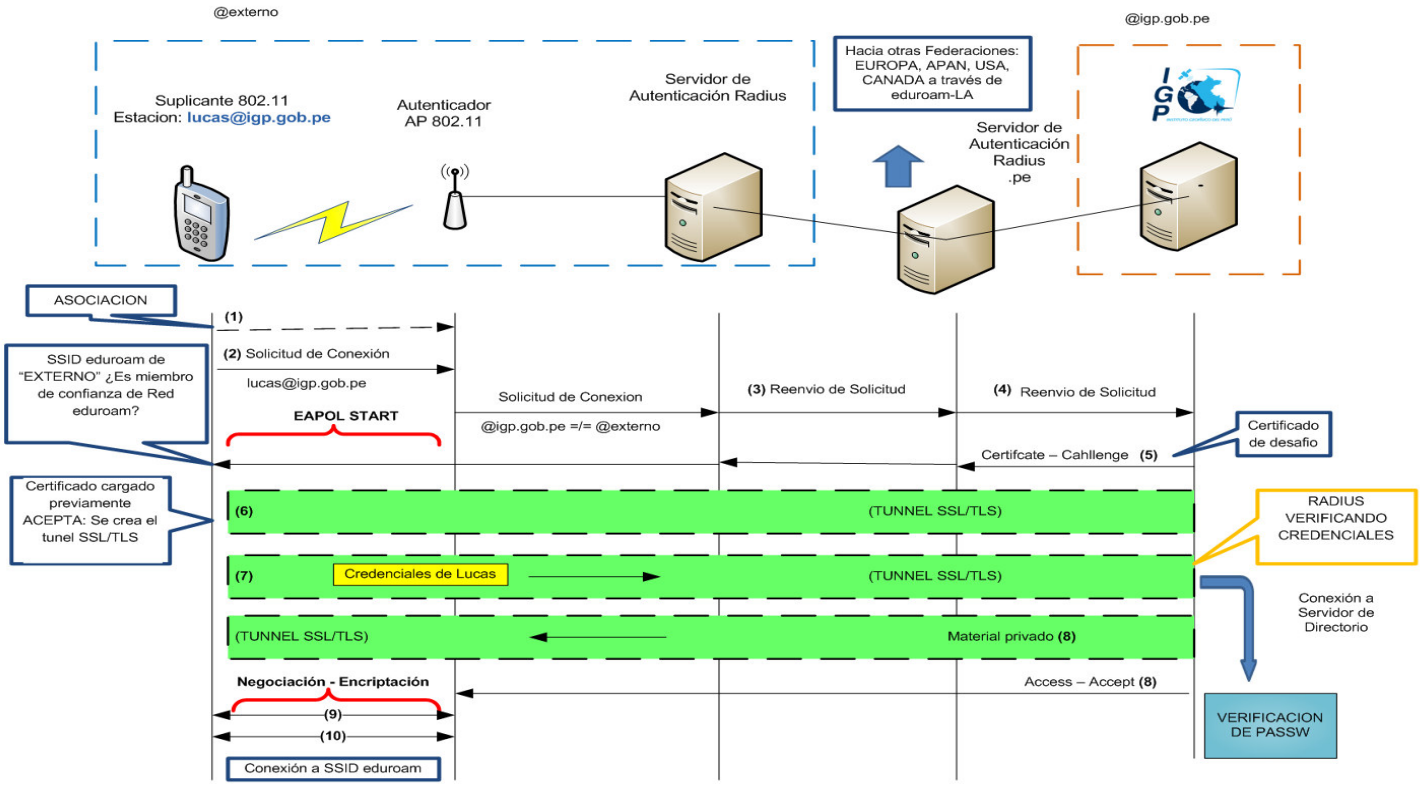


Figura 40: Esquema del proceso de Autenticación en IGP

Fuente:

5.2 Costos de Implementación de la propuesta

Tabla 32.

Especificaciones Técnicas para el modelo de Servidor

Características	Especificaciones Técnicas Requeridas
Procesador	Xeon E5-2640 2.50GHz, 15M cache o superior
Numero de Procesadores	2 procesadores instalados
Tipo de Conjunto Chip	C600 series o superior
Chasis	Hasta 8 Discos Duros de 2.5" (Hot Plug Hard)
Velocidad de Datos	1600 MHz
Configuración de la memoria	Performance Optimizado
Memoria/Tarjeta Gráfica/ Discos	16GB, DDR3 RDIMM Memory, 1600MHz, ECC (2 bancos de 8GB)./ Interno/ Dos (02)
Unidad de disco duro	1TB 7.2K RPM Near-Line SAS 6Gbps 2.5in
Tarjeta controladora	Tarjeta controladora de discos internos que soporte discos SAS, SATA y SSD en RAID 0,1,10,5,50
Panel Frontal	Indicadores LED para el estado del sistema
Puertos, Ranuras	1 x serial – RS-232 – D-Sub de 9 espigas (DB-9) 1 x video VGA – HD – D-sub de 15 espigas (HD-15) 4 x red Gigabit Ethernet 4 x USB (2 frontales, 2 posteriores)

Fuente. Términos de referencia de un proceso del IGP

Tabla 33.

Especificaciones Técnicas para un Punto de Acceso Inalámbrico

Velocidades de datos (Mbps)	802.11b: 1, 2, 5,5, 11 802.11a / g: 6, 9, 12, 18, 24, 36, 48, 54 / 802.11n: 6,5-300 (MCS0 a MCS15)
	802.11ac: 6,5-867 (MCS0 a MCS9, NSS = 1-2)
	Radio de 5 GHz (867 Mbps de velocidad máxima)
	Radio de 2.4-GHz (300 Mbps de velocidad máxima)
	Compuesto con uno de 2 × 2 MIMO y cuatro antenas omnidireccionales downtilt integrados.
Máxima potencia de transmisión	Banda de 2,4 GHz: +21 dBm (18 dBm por cadena)
	Banda de 5 GHz: +21 dBm (18 dBm por cadena)
Bandas de frec.	2.4000 GHz a 2,4835 GHz / 5.150 a 5.850 GHz
Tecnologías de radio soportadas	802.11b: secuencia directa de espectro ensanchado (DSSS) - 802.11a/g/n/ac: (OFDM)
Tipos de modulación	802.11a / g / n / ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM - 802.11b: BPSK, QPSK, CCK
Antena	Ganancia máxima de 4.0 dBi en 2.4 GHz y 6.0 dBi en 5 GHz. Antenas incorporadas están optimizados para techo con orientación horizontal montada del AP.
INTERFACES	10/100 / 1000BASE-T interfaz de red Ethernet (RJ-45)
	Con detección automática de velocidad de enlace y MDI / MDX - 802.3az EEE (Energia Efficient Ethernet)
	PoE-PD: 48 V CC (nominal) PoE 802.3af
	Interfaz de serie de la consola (propietaria; cable adaptador opcional disponible)
Indicadores visuales (LED):	Estado de la energía / sistema
	Estado del enlace Ethernet
	Estado de la radio (dos; RAD0, RAD1)

Fuente. Términos de referencia de un proceso del IGP

Tabla 34.

Especificaciones Técnicas para un conmutador

Características	Especificaciones Técnicas Requeridas
Puertos	48 puertos RJ-45 DE 1/10 SFP+PORT 49 4 puertos QSFP + 40 Gb
Memoria y Procesador	512 de flash tamaño de búfer de paquetes: 9 MB 513 / 2 GB de SDRAM
Estado Latente	10 Gbps Latencia: <1,5 microsiemens
Rendimiento	hasta 952 Mpps
Capacidad de Encaminamiento /	1280 Gbps / Conmutación
Capacidades de Apilamiento	IRF / 4 interruptores
Gestión	Interfaz de línea de comandos, Fuera de la banda de gestión, Administración SNMP, TELNET, FTP
Energía	2 Fuentes de alimentación
Dimensión y Peso	Ancho Profundidad y Altura (43.99 x 65.99 x 4.37 cm) 28,66 Libras (13 kg)
Gestión Capa 3 y Capa 2	Administración de VLAN, soporta de protocolo ARP, Administración de Ethernet Link Aggregation, soporta protocolos STP, IGMP, DHCP, VRRP, y VRRP Administración de protocolo Extendida, Políticas basadas en enrutamiento, ECMP, OSPF, BGP-4, Static IPv6 enrutamiento, Dual IP Stack, OSPFv3, BFG+, IPv6 Tunneling, IPv6.
Seguridad	Soporta configuración de ACL (Listas de Acceso), RADIUS, SSH, Port Security,

Fuente. Términos de referencia de un proceso del IGP

Tabla 35.

En resumen un aproximado mínimo del costo de la implementación

Tipo de equipo	Cantidad	Costo	Costo Total
Servidores de Administración	• 5 (Existen 5 sedes a nivel nacional)	S./ 22 000	S./ 110 000
Equipos de conmutación	• Por cada sede se promedió un mínimo de 5 equipos conmutadores por lo que en total serian 25 equipos conmutadores	S/ 9500	S./ 237 500
Puntos de acceso Inalámbricos	• El requerimiento mínimo por cada sede es de 10 puntos de acceso	S./ 2500	S./ 25 000
Costo Total			S./372 500

Fuente. Cotización dada por J EVANS Y ASOCIADOS S.A.C.

5.3 Beneficios que aporta la Propuesta

❖ **Posibilidad de acceso al usuario visitante**

- Solo un nombre y contraseña
- Acceso a miles de localizaciones
- Configuración de cliente solo una vez
- Fácil de instalar y usar
- Garantiza una seguridad razonable
- Libre de cargo por el uso
- Servicio reciproco significa sin costo a los usuarios
- Integridad de las comunicaciones
- Es un valor agregado en Institución
- Los visitantes pueden usar un servicio simple que facilita la comunicación y conexión a internet
- Permite a sus usuarios el acceso a Internet cuando visiten otra institución de investigación y educación, en el país y en el extranjero

5.3.1 Cronograma de Actividades

Tabla 36.

Cronograma de Implementación del Proyecto de Tesis.

No	ACTIVIDADES:	SEMANAS																																		Total actividad	
		MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE				ENERO				FEBRERO				Semanas	%
		Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6	Semana 7	Semana 8	Semana 9	Semana10	Semana 11	Semana 12	Semana 13	Semana 14	Semana 15	Semana 16	Semana 17	Semana 18	Semana 19	Semana 20	Semana 21	Semana 22	Semana 23	Semana 24	Semana 25	Semana 26	Semana 27	Semana 28	Semana 29	Semana 30	Semana 31	Semana 32	Semana 33	Semana 34	Semana 35	Semana 36	Semana 37	Semana 38	Semana 39	Semana 40		
1	Diseños de TDR para Servidores, Puntos de Acceso, y equipos Conmutadores																																					4	10.0
2	Compra y Adquisicion de equipamiento																																					8	20.0
3	Implementacion del servidor en la sede de Principal de Lima																																					4	10.0
4	Pruebas de verificacion en la sede Principal - La MOLINA																																					3	7.5
5	Pruebas de comunicación en las sedes de Ate, Ancon y Jicamarca																																					2	5.0
6	Planificacion de capacitacion a los Administradores de las remotas de: Huancayo, Arequipa y Chiclayo																																					4	10.0
7	Verificacion del servicio en la sede de Huancayo																																					2	5.0
8	Verificacion del servicio en la sede de Arequipa																																					24	60.0
9	Verificacion del servicio en la sede de Chiclayo																																					3	7.5
10	Verificacion de conectividad entre sedes a nivel Nacional																																					2	5.0
11	Coordinacion con INICTEL para la autorizacion de los servicios eduroam																																					28	70.0
	TOTAL:																																					40	100%

Fuente. Datos planificados por área de Tecnologías del IGP

CONCLUSIONES

El desarrollo de la tecnología inalámbrica abre un sin fin de alternativas para el despliegue de las comunicaciones sea con el uso de distintos dispositivos otorgando accesibilidad y escalabilidad a la red. Esto incluye procesos de autenticación y autorización con el uso del protocolo RADIUS (Remote Authentication Dial In User Service). A lo largo del trabajo se ha mostrado los diferentes mecanismo de protección y el salvaguardar la información que implica el uso de estándares de seguridad, el uso del protocolo AAA (Autenticación, Autorización y Administración) usado para las aplicaciones que utilicen dispositivos móviles y a su vez lo utiliza RADIUS. EL AAA también un protocolo de autenticación utilizado por el estándar de seguridad del 802.1x (Redes inalámbricas) haciendo referencia a los métodos de autenticación con el uso del protocolo EAP en sus diferentes modos tales como: EAP – TLS, EAP-TTLS, EAP-PEAP.

Los parámetros que utilizan los procesos de Autenticación y Autorización al acceso de la red local, permiten tener un control más detallado del usuario llegando a identificar el grado de procedencia del invitado.Permitir al sistema inalámbrico el uso del protocolo RADIUS con la aplicación eduroam brinda un valor agregado a la institución catalogándola como una Institución de confianza a nivel internacional, y a su vez los usuarios dispondrán de acceso a este servicio fuera de la institución de origen. La percepción de los usuarios al hacer uso de la aplicación eduroam permitió conocer las bondades inherentes tales como el Acceso a entidades externas y sus recursos disponibles, control de tráfico para el administrador de Red de la Institución y libre de costos fuera de la institución de origen a Internet.

RECOMENDACIONES

En base a la propuesta diseñada es necesario desarrollar un plan de trabajo, realizando un análisis donde los recursos tecnológicos soporten nuevas tecnologías basándose en la escalabilidad de la red y teniendo en cuenta la seguridad informática.

Por otro lado conocer la realidad y la perspectiva de los usuarios de modo que al proponer una mejora para la Institución deba ser aceptada por todos los empleados y tenga el respaldo de la Alta Dirección. Es así que la información proporcionada por distintas áreas será analizada y podremos constatar el impacto que esta implementación generara en las diversas necesidades funcionales de los empleados de la Institución.

La implementación debe ser progresiva y consensuada con la Alta dirección y las áreas donde se va a disponer, esta implementación a nivel nacional debe tener un estudio de campo el cual en coordinación con la sede Principal en Lima otorgue las validaciones para que estos servicios se encuentren activos y autorizados en las confederaciones a nivel internacional.

Este servicio debe masificarse a nivel nacional en todas las instituciones de Investigación.

REFERENCIAS BIBLIOGRAFICAS

AAA Radius and Diameter Server Market Shares Strategies, and Forecasts, 2009 to 2015 from http://wintergreenresearch.com

Carbonell, X. T. (2013). Cómo conocer el uso actual de las redes WLAN basadas en IEEE 802.11

Cisco. (2006). ¿Cómo el RADIUS trabaja?. , Recuperado de: http://www.cisco.com/c/es_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html.

Cisco. (2017). Chapter: Authentication in ACS 5.2, Recuperado de: http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-2/user/guide/acsuserguide/eap_pap_phase.html

El Yaagoubi, M. (2012). Acceso a Internet vía WiFi-WiMax, Recuperado de: http://e-archivo.uc3m.es/bitstream/handle/10016/15906/pfc_mohammed_el-yaagoubi_2012.pdf

Eduroam Service Definition and Implementation Plan. GEANT. (2017). *Deliverable DS5.1.1*, from https://www.eduroam.org/support/eduroam-documentation/

FUNET. (2003). *Aplicación del acceso público basado en radios en Roaming. La Red Universitaria Finlandesa (FUNET)* Finlandia:

Institute of Communications Engineering Korkeakoulunkatu 1, 33720 Tampere, Finland.

Gonzales, R. I. (2017). Despliegue del Servicio EDUROAM en el Campus Universitario de la UNMSM. Recuperado de: http://documentos.redclara.net/bitstream/10786/974/1/126-Despliegue%20del%20Servicio%20eduroam.pdf

Huhtanen, K., Vatiainen, H., Keski-Kasari, S., & Harju, J. (2010). *Implementing multi-federation and peer-to-peer roaming on the eduroam federation level, Living the network life*. Paper presented at the The 22th Trans European Research and Education Networking Conference, Vilnius, Lithuania.

INICTEL. (2014). *Manual de instalación y configuración (v3.0) para nodos pilotos de eduroamLA. - Configuración Básica del RADIUS Local*: Instituto Nacional de Investigación y Capacitación de Telecomunicaciones

INICTEL. (2014). *Manual de Instalación y configuración (v3.0) para nodos pilotos de eduroam-LA. Protocolo LDAP y LOGs*.

INICTEL. (2014). Manual de instalación y configuración (v3.0) para nodos pilotos de eduroam-LA. Servidor Redes Inalámbricas IEEE 802.11

INICTEL. (2014). *Manual de Instalación y configuración (v3.0) para nodos pilotos de eduroam-LA*: Instituto Nacional de Investigación y Capacitación de Telecomunicaciones INICTEL

Leonardo, J. (2014). Principales dificultades del sistema de seguridad y protección del centro histórico de la Ciudad de Holguín. Colombia. Recuperado de: http://gruespac-espe.blogspot.pe/2009/05/seguridad-una-introduccion-dr.html

LDAP – Dany Conte Jan 2002. Conte Consultans Inc. . from www.conte.on.ca

Manunta, G. (2006). Seguridad: Una Introducción *Revista Virtual Seguridad Corporativa.* Recuperado de: http://www.belt.es/bibliografia/HOME2_articulo.asp?id=130.

Microsoft. (2016). Decision Source: TRM Mgmt Group Decision Process:One-VA TRM v16.6 Decision, from https://www.va.gov/TRM/

Milinovic, M., Penezić, D., Thomson, I., & group, S. (2008). Deliverable DS5.3.1: Report on Introduction of Monitoring System and Diagnostics Tools April 2008 from https://www.eduroam.org/support/eduroam-documentation/

Milinovic, M., Penezić, D., Thomson, I., & group, S. (2008). Deliverable DS5.3.1: Report on Introduction of Monitoring System and Diagnostics Tools April 2008 from https://www.eduroam.org/support/eduroam-documentation/

palabra, T. h. (2007). EAP: Extensible Authentication Protocol, Recuperado de: http://www.tecnologiahechapalabra.com/ciencia/miscelanea/articulo.asp?i=724

Protocolos de seguridad de ingeniería con ModelChecking - Radius-SHA256 y protocolo Simple protegido (2017), from http://www.mdx.ac.uk

Quinto, J. R., Leiva, A. M., & Quiroz, J. L. (2017). Propuesta de una infraestructura segura para el monitoreo de eventos en eduroam Latinoamérica

Revolvy. (2017). A network access server (NAS) is a single point of access to a remote resource. Recuperado de: https://www.revolvy.com/main/index.php?s=Network%20access%20server

Remote Authentication Dial In User Service (RADIUS) Network Working Group C. . from https://tools.ietf.org/html/rfc2865

Searchmobilecomputing. (2017). Definition 802.1X., Recuperado de: http://searchmobilecomputing.techtarget.com/definition/8021X

Technet. (2017). Capacidad de OI: Seguridad y funciones de red: del nivel estandarizado al racionalizado. Recuperado de: https://technet.microsoft.com/es-es/library/bb821287.aspx

TECSUP. (2013). *Programa Integral "Seguridad de Sistemas de la Información* Lima, Perú: Programa de Capacitación Continua. Departamento de Informática Tecsup.

T. Lenggenhager, T., Winter, S., T. Wolniewicz, T., D. Lopez, D., S. Neinert, S., J. Rauschenbach, S.I. Thomson, I. (2008). Advanced Technologies Overview, from https://www.eduroam.org/support/eduroam-documentation/

TELEM@TICA. (2015). Control de Acceso a la Red WIFI de la UCLV. . *Revista digital de las tecnologías de la información y las comunicaciones.* , Año VII No. 20 ISSN: 1729-3804. Recuperado de: https://www.fiec.espol.edu.ec/resources/download/revista/Telematica_A%C3%B1oVII_No20.pdf.

Vázquez, S. M. (2014). *Estudio técnico y diseño para el despliegue de una red de banda ancha inalámbrica en el cantón chordeleg usando tecnología de acceso wi-fi en distintos puntos del cantón y dentro de la i. municipalidad de chordeleg.* Universidad de Cuenca, Ecuador.

Ventura, Y. L. (2008). *Diseño y desarrollo de honeynets virtuales utilizando VMWARE, para la detección de intrusos informáticos.* Universidad Francisco Gavidia., San Salvador.

Vidal, L. H. (2009). *ICIHONEY: Diseño e Implementación de una Red Trampa en el Instituto de Informática de la Universidad Austral de Chile. .* Universidad Austral de Chile Valdivia, Chile. .

what-when-how. (2017). Layer 3 To Linearity (Technology Terms) Recuperado de: http://what-when-how.com/technology-terms/layer-3-to-linearity-technology-terms/

Winter, S., Milinovic, M., & Thomson, I. Deliverable DS5.4.1: Report on RadSec Integration from https://www.eduroam.org/support/eduroam-documentation/

ANEXOS

ANEXO A: TABLAS DE ANALISIS ESTADISTICOS DE FRECUENCIAS SOBRE LAS VARIABLES – SPSS 20

Tabla 37.

Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	En poca Medida	1	2,5	2,5	2,5
	En alguna Medida	18	45,0	45,0	47,5
	En gran Medida	21	52,5	52,5	100,0
	Total	40	100,0	100,0	

Fuente. IGP-Encuesta virtual

Tabla 38.

Grado de autenticación del control del tráfico inalámbrico

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	En poca Medida	3	7,5	7,5	7,5
	En alguna Medida	21	52,5	52,5	60,0
	En gran Medida	15	37,5	37,5	97,5
	Totalmente	1	2,5	2,5	100,0
	Total	40	100,0	100,0	

Fuente. IGP-Encuesta virtual

Tabla 39.

Grado de autorización del control del tráfico inalámbrico

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	En poca Medida	1	2,5	2,5	2,5
	En alguna Medida	19	47,5	47,5	50,0
	En gran Medida	20	50,0	50,0	100,0
	Total	40	100,0	100,0	

Fuente. IGP-Encuesta virtual

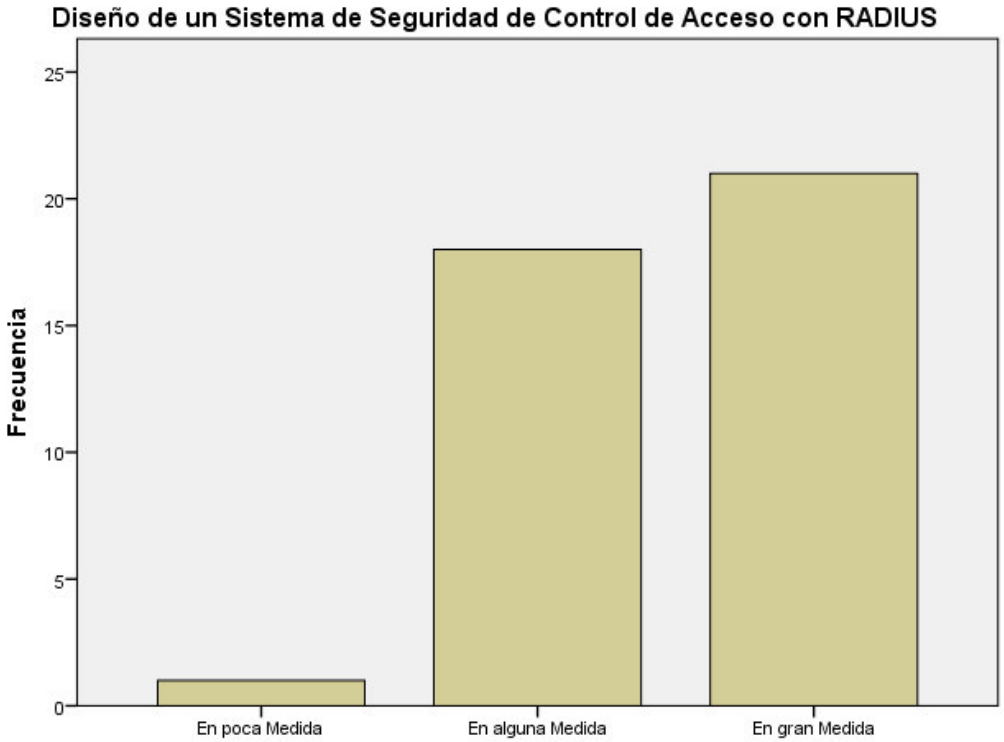


Figura 41: **Estadísticas de Frecuencias de Un Sistema de Seguridad de Control de Acceso con RADIUS**
Fuente. IGP-Encuesta virtual

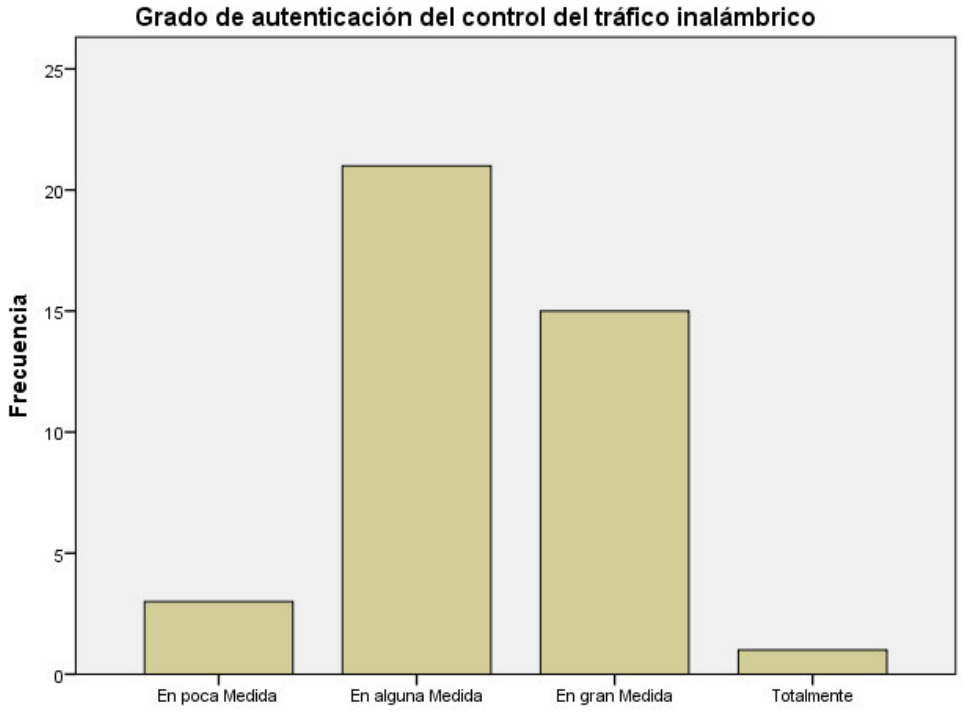


Figura 42: **Frecuencias del Grado de Autenticación del control de Trafico Inalámbrico**
Fuente. IGP-Encuesta virtual

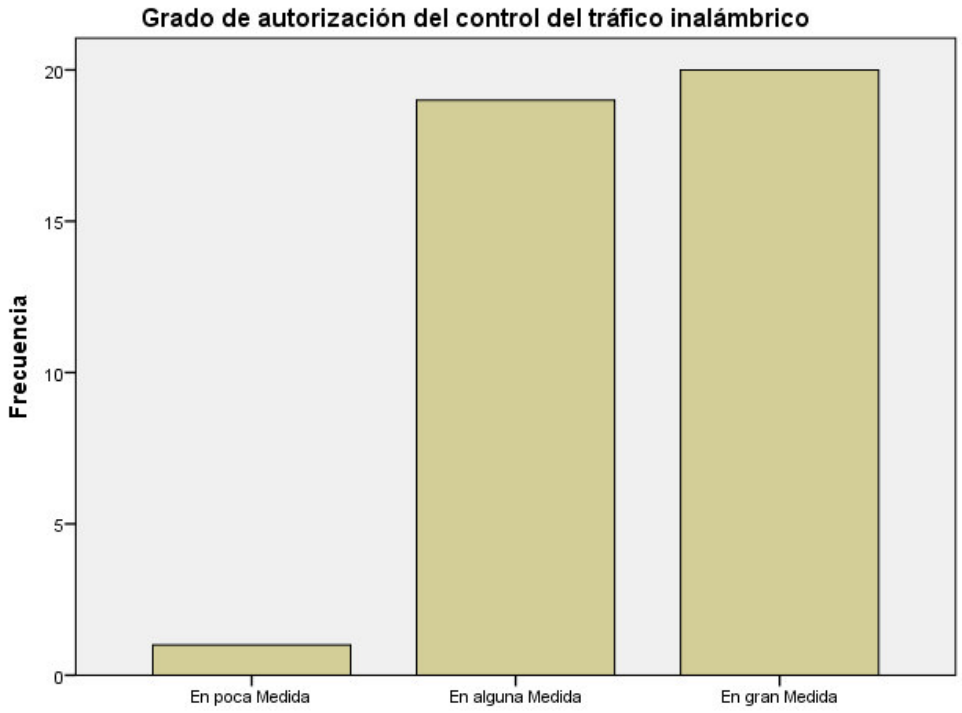


Figura 43: **Estadísticas de Frecuencias del Grado de Autorización del control del Tráfico inalámbrico**
Fuente. IGP-Encuesta virtual

ANEXO B: ANALISIS DESCRIPTIVOS DE LAS VARIABLES

Tabla 40.
Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. típ.
Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS	40	2	4	3,50	,555
Grado de autenticación del control del tráfico inalámbrico	40	2	5	3,35	,662
Grado de autorización del control del tráfico inalámbrico	40	2	4	3,48	,554
N válido (según lista)	40				

Fuente. IGP-Encuesta virtual

ANEXO C: ANÁLISIS ESTADÍSTICO DE LAS MEDIAS

Tabla 41.
Resumen del procesamiento de los casos

	Casos					
	Incluidos		Excluidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Grado de autenticación del control del tráfico inalámbrico * Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS	40	100,0%	0	0,0%	40	100,0%
Grado de autorización del control del tráfico inalámbrico * Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS	40	100,0%	0	0,0%	40	100,0%

Fuente. IGP-Encuesta virtual

Tabla 42.
Informe estadístico

Sistema de Seguridad con RADIUS		Grado de autenticación del control del tráfico inalámbrico	Grado de autorización del control del tráfico inalámbrico
En poca Medida	Media	3,00	3,00
	N	1	1
	Desv. típ.	.	.
	Varianza	.	.
En alguna Medida	Media	2,94	3,33
	N	18	18
	Desv. típ.	,539	,594
	Varianza	,291	,353
En gran Medida	Media	3,71	3,62
	N	21	21
	Desv. típ.	,561	,498
	Varianza	,314	,248
Total	Media	3,35	3,48
	N	40	40
	Desv. típ.	,662	,554
	Varianza	,438	,307

Fuente. IGP-Encuesta virtual

Tabla 43.
Tabla de ANOVA

			Suma de cuadrados	gl	Media cuadrática	F	Sig.
Grado de Autent. del control del tráfico inalámbrico * Sistema de Seguridad con RADIUS	Inter-grupos	(Combinadas)	5,870	2	2,935	9,670	,000
		Linealidad	5,333	1	5,333	17,572	,000
		Desviación de la linealidad	,537	1	,537	1,768	,192
	Intra-grupos		11,230	37	,304		
	Total		17,100	39			
Grado de Autoriz. Del control del tráfico inalámbrico * Sistema de Seguridad con RADIUS	Inter-grupos	(Combinadas)	1,023	2	,511	1,727	,192
		Linealidad	1,021	1	1,021	3,449	,071
		Desviación de la linealidad	,002	1	,002	,006	,939
	Intra-grupos		10,952	37	,296		
	Total		11,975	39			

Fuente. IGP-Encuesta virtual

Tabla 44.
Medidas de asociación

	R	R cuadrado	Eta	Eta cuadrado
Grado de autenticación del control del tráfico inalámbrico * Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS	,558	,312	,586	,343
Grado de autorización del control del tráfico inalámbrico * Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS	,292	,085	,292	,085

ANEXO D: ITINERANCIA EN EL SERVICIO EDUROAM

Panorama de puntos eduroam a nivel Internacional

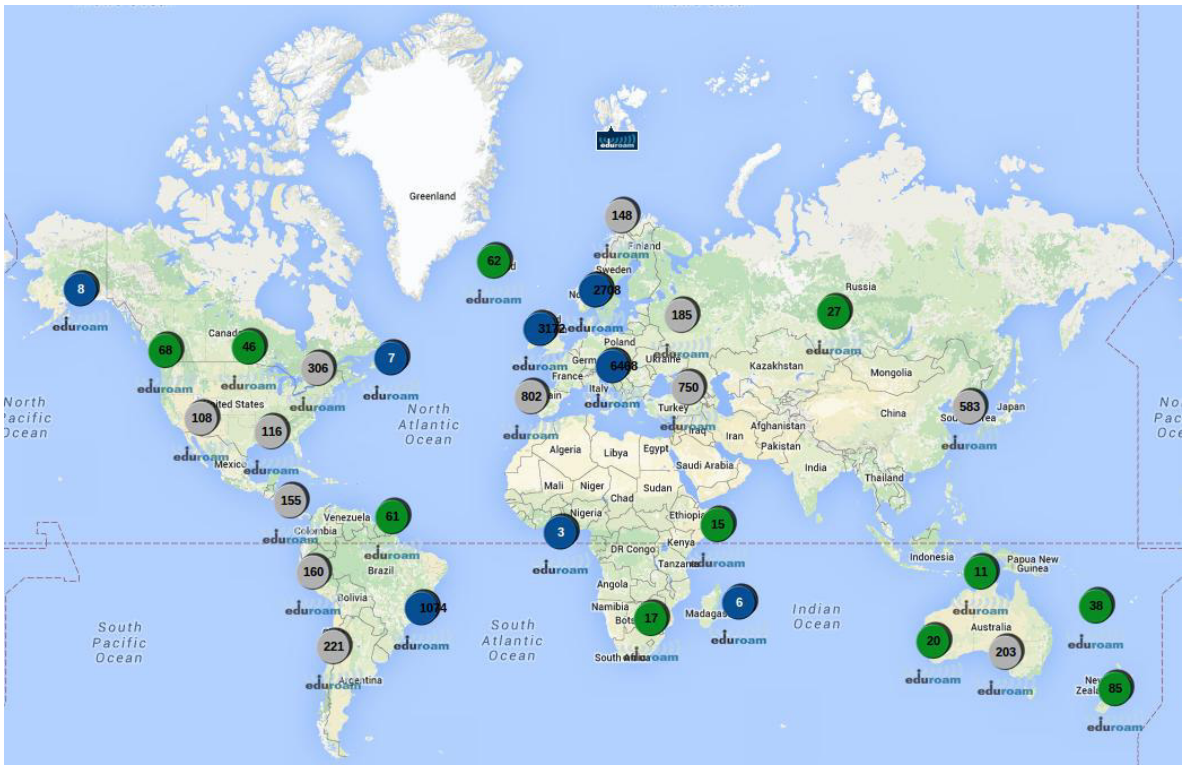


Figura 44: **Acceso al servicio eduroam a nivel internacional.**

Fuente. eduroam.org

Itinerancia en España:

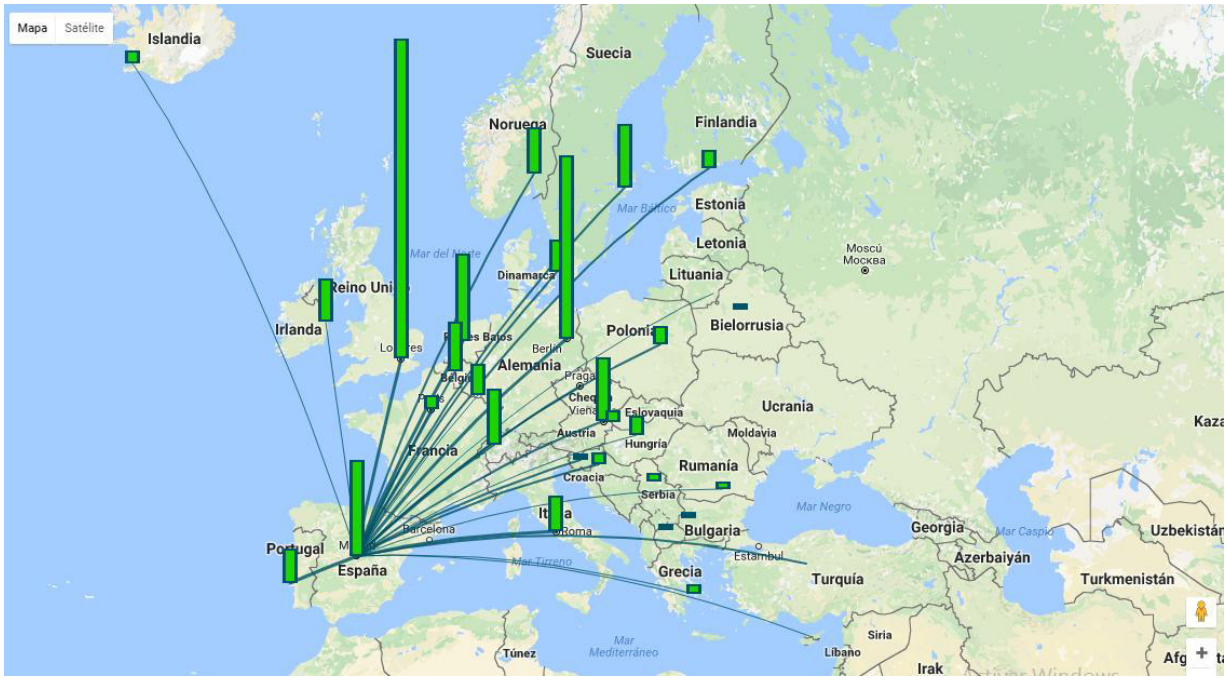


Figura 45. **Itinerancia eduroam en España**

Fuente: eduroam.org

Itinerancia en Inglaterra:

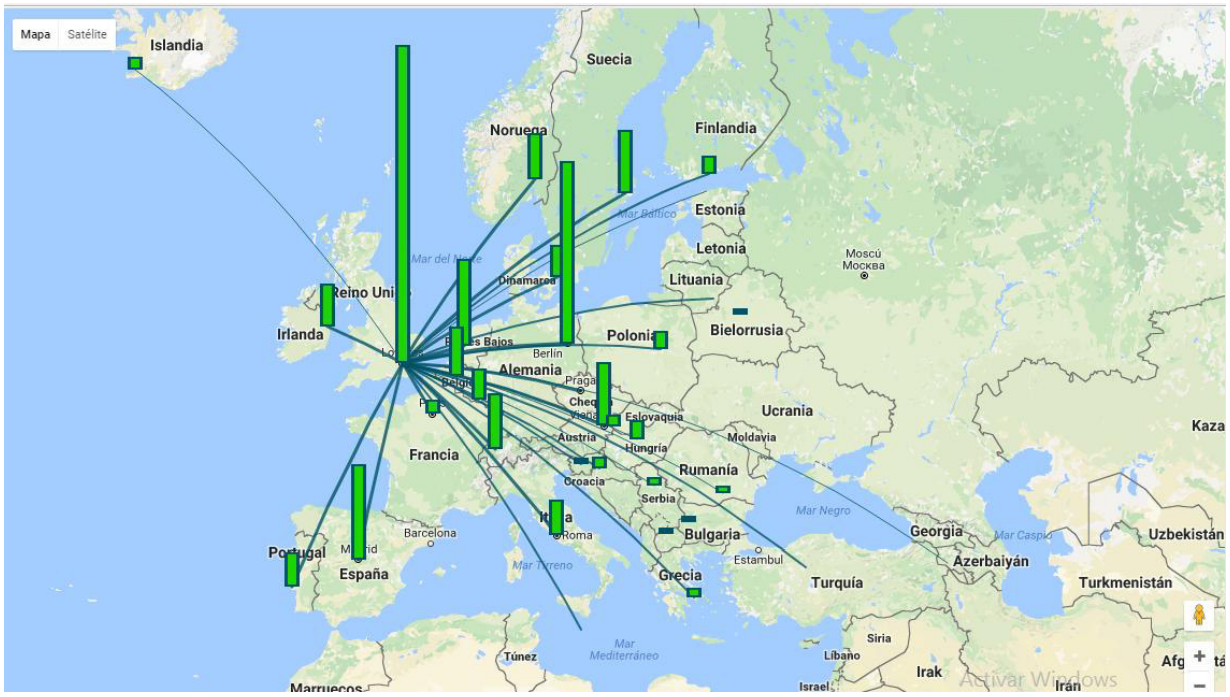


Figura 46. **Itinerancia eduroam en Reino Unido.**

Fuente. eduroam.org

ANEXO E: POSIBLES TECNOLOGÍAS ALTERNATIVAS PARA EDUROAM-NG

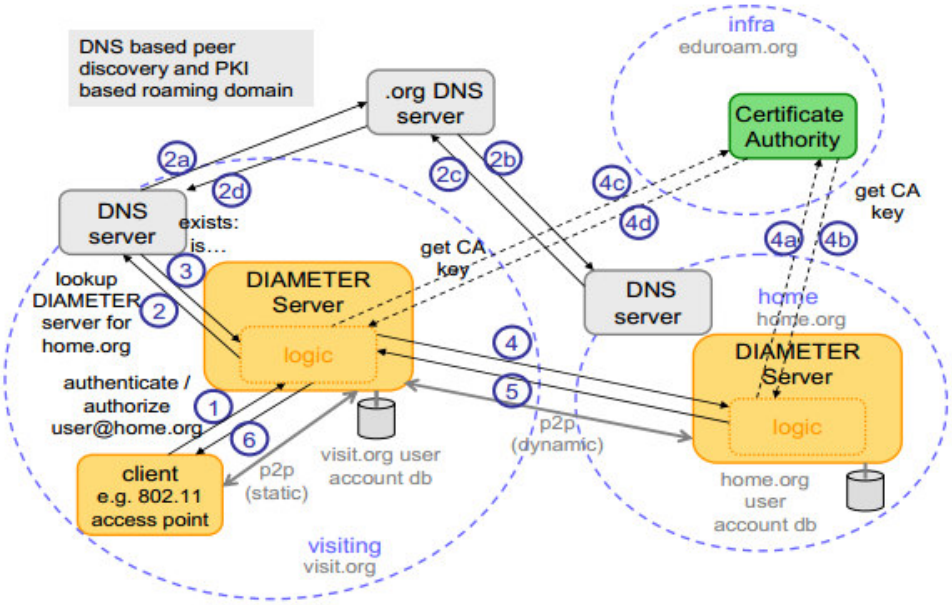


Figura 47. **Itinerancia Diameter con DNS 3.1**

Diameter and RADIUS legacy connections

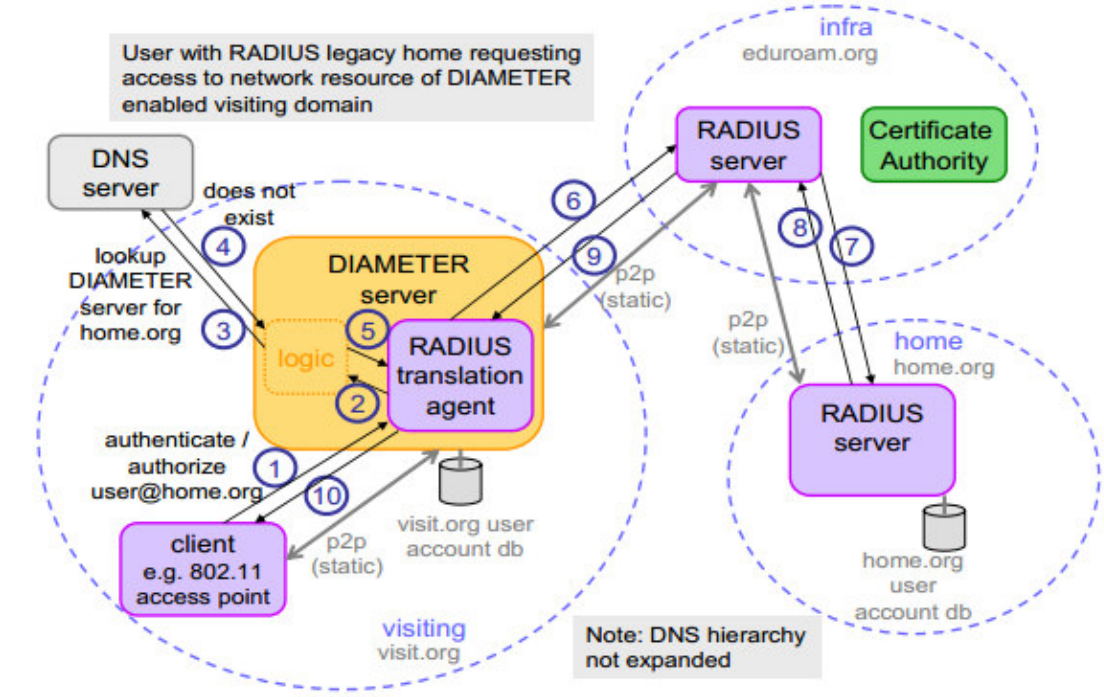


Figura 48. **Diámetro con legado RADIUS: Comunicación entre pares basada en RADIUS**

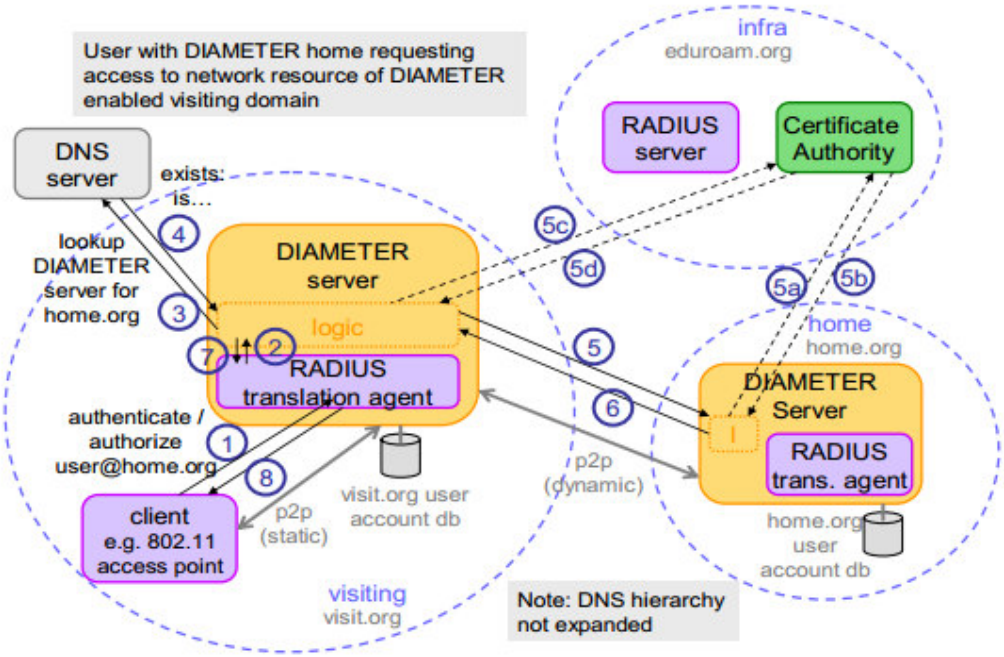


Figura 49: **Diámetro con legado RADIUS: Comunicación por pares basada en diámetro**

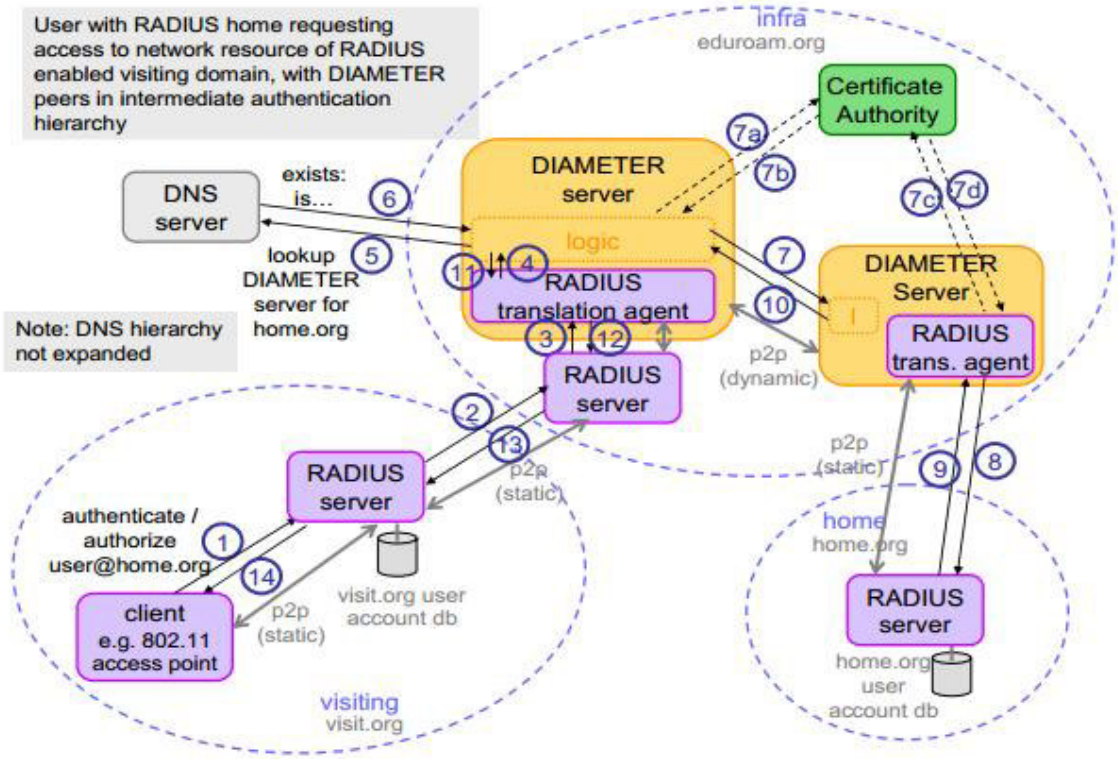


Figura 50: **RADIUS mixto / Diámetro, RADIUS menor en jerarquía, Diámetro más arriba**

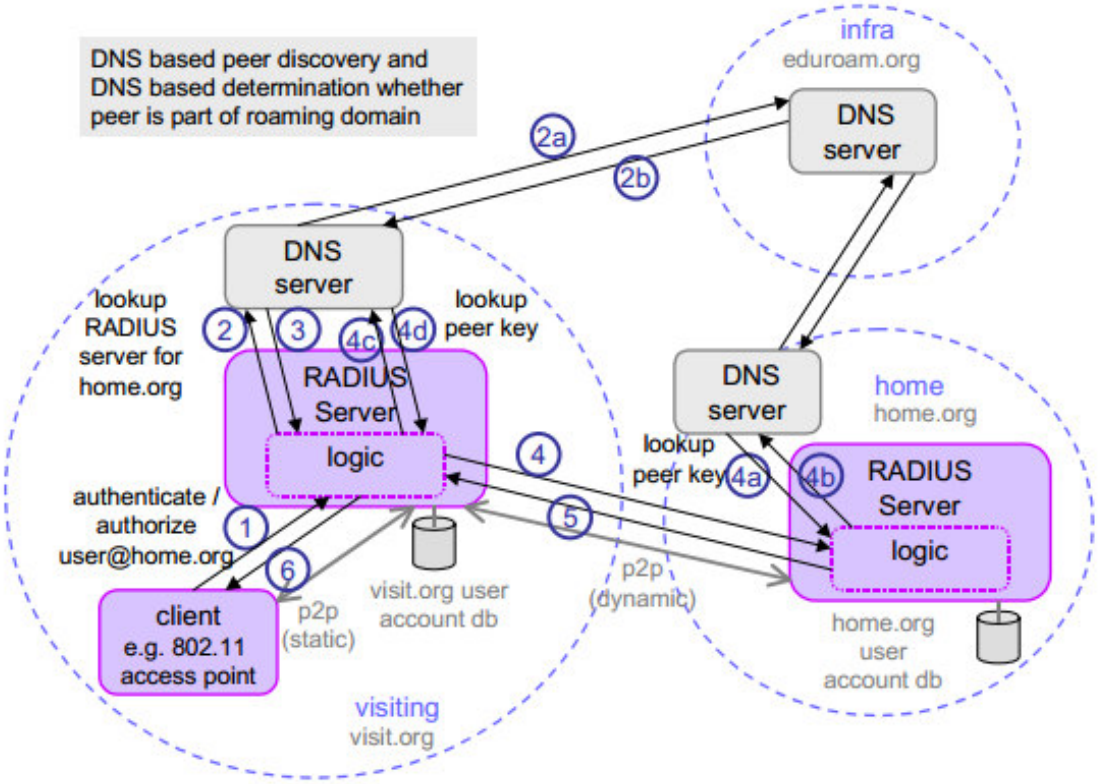


Figura 51. **RADIUS-DNSSEC roaming model**

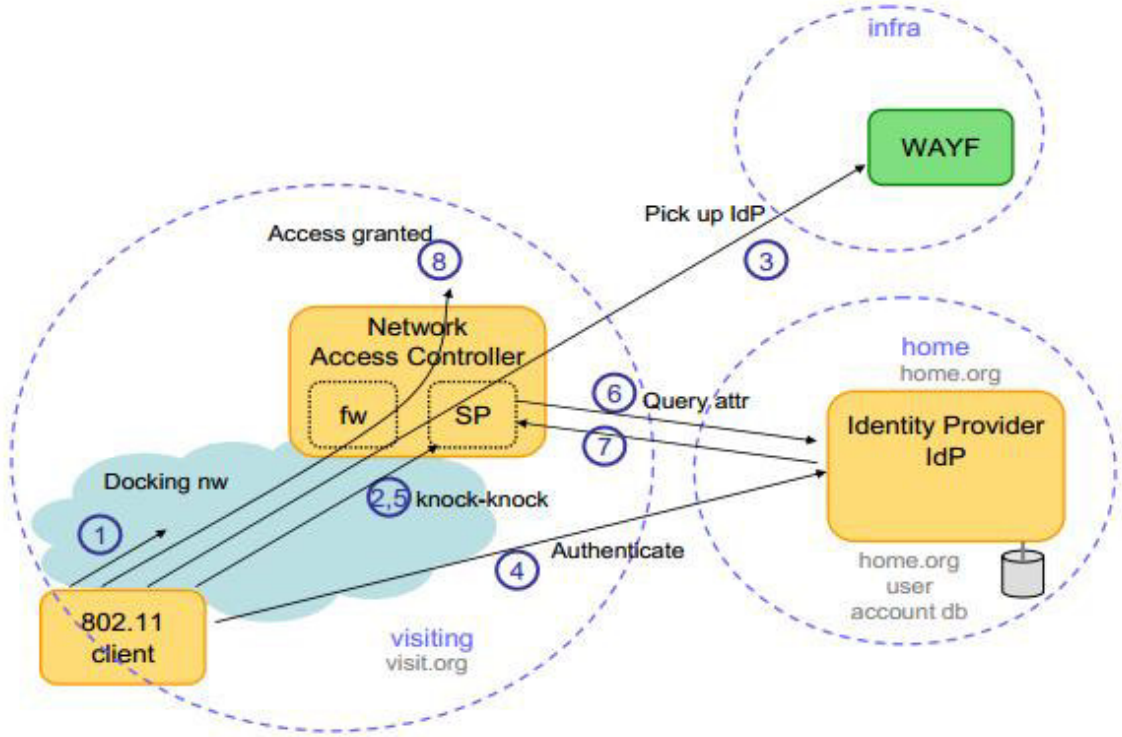


Figura 52. **Modelo de itinerancia basado en redirección web y AAI.**

ANEXO D: FUNCIONAMIENTO DEL SERVICIO

Los usuarios que soliciten acceso al servicio eduroam, informaran a la Oficina de Tecnologías quienes a su vez otorgaran un usuario y contraseña que serán las credenciales del correo electrónico

Tabla 45. Datos de Usuario eduroam

Usuario	lcastillo@igp.gob.pe
Contraseña	aoukac37

Los dispositivos moviles podrán acceder al servicio eduroam al encontrar cualquier señal con el SSID: “eduroam”: Acceso desde un smarthpone

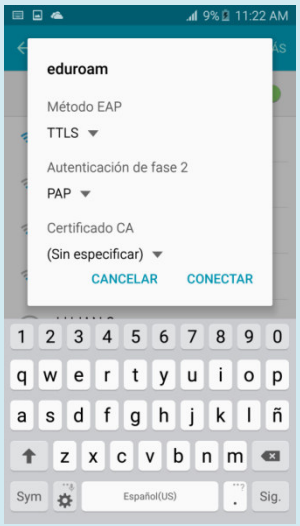
Android	Iphone (solo usuario y password)
	

Figura 53. **Configuración en dispositivos móviles servicio eduroam.**

Figura 54: **Configuración de acceso eduroam en Mac O.S.**

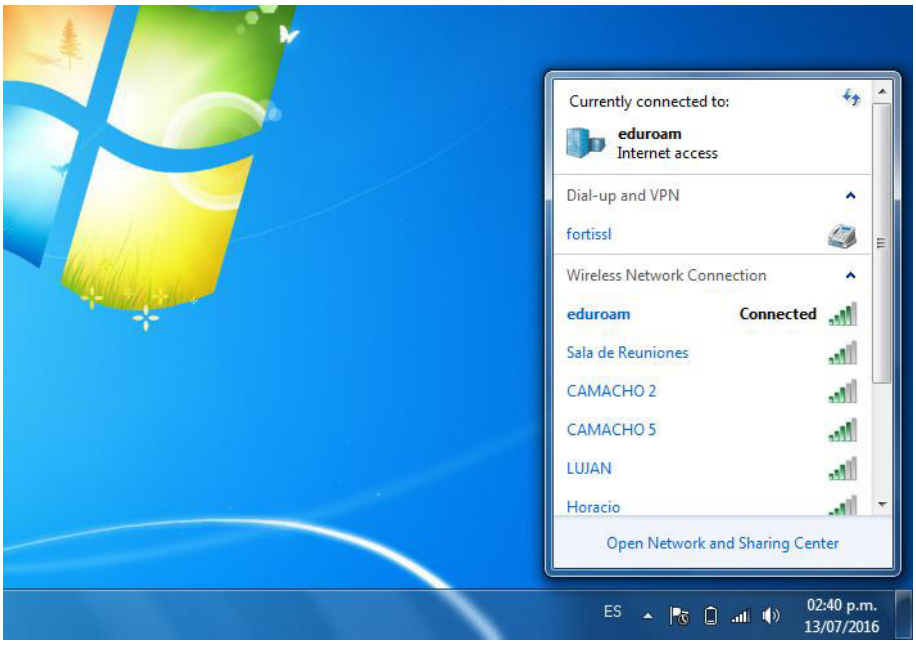


Figura 55. **Configuración de acceso eduroam en Windows**

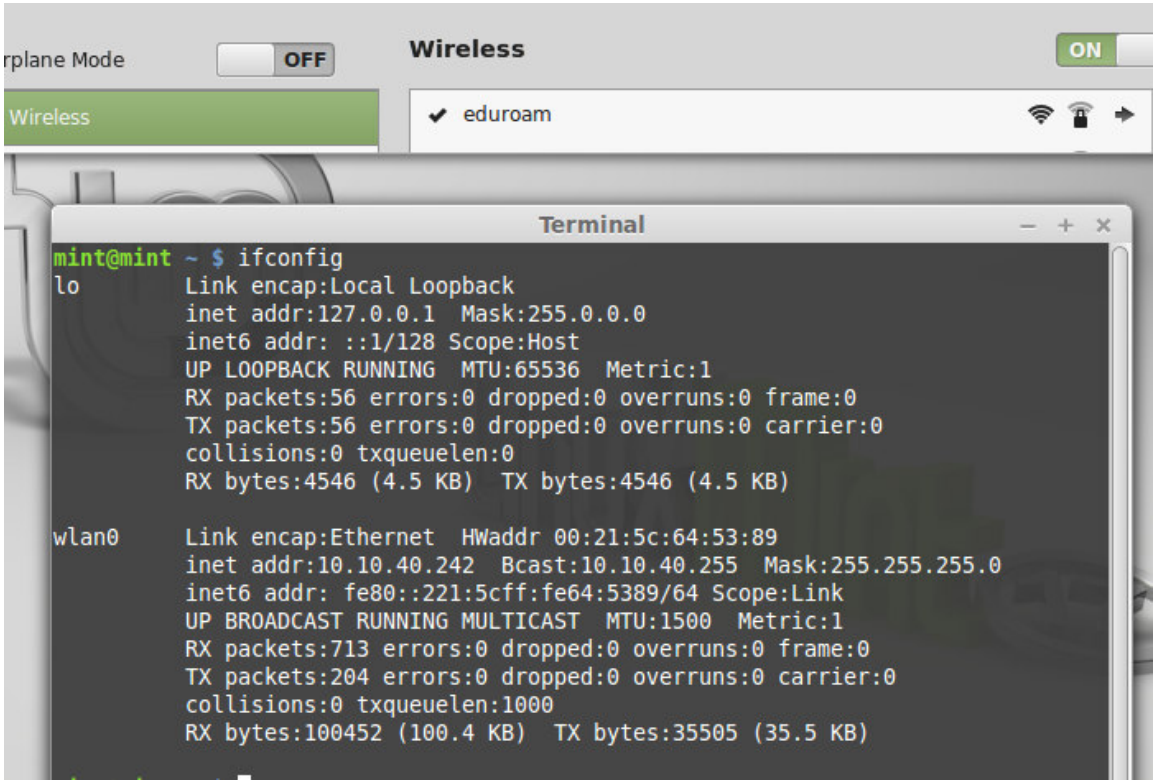


Figura 56: **Configuración de acceso eduroam en LINUX**

.